PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

MARINA KRONEMBERGER DOS SANTOS

Vigilância e Tecnocontrole: a Arquitetura de Dissolução da Privacidade e a Degradação da Democracia

LUCIANA BADIN
ORIENTADORA

Rio de Janeiro

2020.2

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

MARINA KRONEMBERGER DOS SANTOS

Vigilância e Tecnocontrole: a Arquitetura de Dissolução da Privacidade e a Degradação da Democracia

Monografia apresentada ao Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) como requisito parcial para obtenção do título de Bacharel em Relações Internacionais.

LUCIANA BADIN
ORIENTADORA

SÉRGIO VELOSO
SEGUNDO LEITOR

Rio de Janeiro

2020.2

AGRADECIMENTOS

Tenho uma sorte tremenda por ter um grupo tão amoroso e atencioso me apoiando ao longo da graduação e dos últimos anos. Gostaria, então, de agradecer à minha família, aos meus amigos, à Pontifícia Universidade Católica – especialmente ao Instituto de Relações Internacionais – e aos meus colegas de trabalho da IBM.

Aos meus pais e meu irmão, obrigada por me apoiar e incentivar sempre. Vocês são o motivo por eu estar aqui hoje.

À minha família no Rio: Tia Ana, Dominique e Tia Bel, obrigada por todo o carinho, torcida e por me acolherem.

Aos meus amigos. Bia e Pedro, amo vocês demais e sua torcida é realmente especial. Giulia N., Juliana, Giulia R. e Maria Beatriz, vocês alegram minhas manhãs e estão lá para todos os surtos e vitórias, obrigada por tudo!

À PUC e ao IRI: nos últimos quatro anos conheci pessoas incríveis que me ensinaram muito e me abriram os olhos para vários problemas. Em especial, gostaria de agradecer à minha orientadora Luciana Badin por todos os ensinamentos e principalmente pelo apoio no último ano. Ao professor Sérgio Veloso por me introduzir ao trabalho tão importante da Shoshana Zuboff e sempre nos forçar a pensar além da nossa "bolha." Aos professores Ricardo Oliveira, Márcio Scalercio, Marcello Cappucci, Diego Santos, Paula Drumond, Manuela Trindade, Renata Summa, agredeço imensamente por compartilharem sua sabedoria e por todo o carinho e atenção.

Aos colegas da IBM: Thiago, Julia, Maysa, Gabrielle, Julio, Juliana, Lavínia, Lis, Vitória, Bruno, obrigada por tudo! Aprendi demais com vocês nesses dois anos.

RESUMO

Em meio a uma pandemia que exige o distanciamento social como uma forma de deter o avanço do Covid-19, a tecnologia se tornou um grande aliado para dar continuidade ao trabalho, estudos, convívio social e mais. No entanto, tudo que fazemos em aparelhos conectados à Internet é monitorado por algumas empresas, o que colabora para a disseminação de um ambiente de vigilância permanente, uma vez que cada vez mais somos dependentes da tecnologia. O presente trabalho visa examinar tais mecanismos envolvidos na captação, controle e compartilhamento de dados pessoais com o objetivo de compreender como o direito à privacidade é violado nesse processo e quais as consequências sobre a vida em sociedade, especialmente quanto ao livre funcionamento da democracia. Por meio de uma análise das operações do Google e do Facebook**,** pretendemos mostrar como essas empresas instituíram e disseminaram um novo modelo econômico que sistematicamente desrespeita a privacidade, perpetua o racismo e anula as subjetividades, padronizando o comportamento e degradando a democracia. Ademais, dada essa assimetria de informação e de poder em favor das *big tech*, julgamos necessário pensar em maneiras de resistir a esse sistema. E, portanto, mostraremos como mobilizações no âmbito privado, no aparato legal e na sociedade civil têm sido implementadas nos últimos anos para lutar contra as amarras do capitalismo de vigilância.

PALAVRAS-CHAVE: privacidade; capitalismo de vigilância; tecnocontrole; democracia.

SUMÁRIO

Introdução

Vivemos em um mundo onde aqueles sem uma conta de *e-mail* são invisibilizados, mas principalmente onde as redes sociais e a Internet em geral tornam a ansiedade soberana. Nesse mesmo mundo, os dados são uma mercadoria. Se você possui uma conta de *e-mail*, rede social, aplicativo de transporte, de entretenimento, de relacionamento ou mesmo bancário, muito provavelmente suas informações pessoais estão sendo comercializadas sem o seu consentimento nesse instante. Em troca, você recebe os "melhores" resultados nos sites de pesquisa, bem como o bombardeio diário de mais de 5 mil propagandas no seu *feed*. A este processo é dado o nome de "capitalismo de vigilância."

Para Shoshana Zuboff (2018), filósofa e professora emérita da Harvard Business School, trata-se de um ciclo na lógica de acumulação mediada por computador: primeiro, há a produção do dado mediante a ação do usuário; em seguida, as informações são coletadas e analisadas, para então, retornarem ao usuário como propaganda. Assim, conforme cada vez mais objetos do cotidiano estão conectados à Internet e aspectos da vida como trabalho, lazer e educação se tornam mais dependentes da conectividade – especialmente com a atual pandemia do novo corona vírus – mais os indivíduos se tornam mais padronizados e as subjetividades se perdem (ZUBOFF, 2018, p. 27-34), num processo permeado pela constante violação da privacidade do indivíduo. Isto é, segundo a professora de Direito da PUC-Rio Caitlin Mulholland,

> Fato é que nossa sociedade atual é fundamentada num modelo de regulação tecnológica ineficiente que gera, por sua vez, a possibilidade de mercantilização de dados pessoais sem que haja um adequado aparato legal capaz de proteger o direito fundamental à privacidade (MULHOLLAND, 2019, p. 11).

Diante do quadro acima, o presente trabalho busca investigar os mecanismos envolvidos na captação, controle e compartilhamento de dados pessoais capturados por mecanismos de vigilância, de forma a compreender como o direito à

privacidade é violado nesse processo e quais as consequências sobre a vida em sociedade, especialmente quanto aos fundamentos da democracia.

Como sustenta Helen Nissenbaum, professora da Cornell Tech e diretora do Digital Life Initiative, em entrevista à série documental *Expresso Futuro* (2018), não se trata de debater o *trade-off* entre fluxo de dados e privacidade, pois isto coloca a privacidade em uma posição muito difícil de defender, já que a primeira categoria traz uma imensidão de benefícios. Trata-se de um fluxo apropriado e transparente, no qual os termos e condições sejam claros. Afinal, dados são como um bem coletivo, na medida em que regulam a relação entre o governo e a população. Dessa forma, devem servir à sociedade de forma a melhorar nossa experiência enquanto cidadãos e usuários (EXPRESSO FUTURO, 2018).

Assim sendo, ao mesmo tempo em que a privacidade deve ser protegida, os usuários também desejam e devem desfrutar dos benefícios advindos da tecnologia. Portanto, é necessário que tenham acesso às informações coletadas pelos serviços digitais que utilizam, assim como a capacidade de decidir o que é feito com elas e desfrutar de possíveis lucros advindos de alguma troca comercial, exercendo plenamente sua autodeterminação informativa (MULHOLLAND, 2019, p. 15-6).

Portanto, diante de um cenário onde temos de abrir mão de parte da nossa liberdade em prol da participação no mundo virtual, o mérito desta pesquisa está em mapear os meios pelos quais o capitalismo de vigilância opera atualmente de forma a identificar as consequências impostas sobre a sociedade, em especial quanto à violação da privacidade e ao pleno funcionamento da democracia.

Para concretizar esse objetivo, a pesquisa está estruturada em quatro movimentos analíticos. Num primeiro momento, será realizada uma análise histórica do conceito de privacidade de forma a compreender como este evoluiu ao longo do tempo para ser entendido como um direito fundamental, mas é sistematicamente violado pelo capitalismo de vigilância.

Na primeira seção, a privacidade será analisada a partir principalmente das contribuições de James Madison e John Locke, observando como a princípio o conceito foi interpretado na lei norte-americana como uma forma de proteção da

propriedade dos indivíduos. Em seguida, devido à sua proximidade na literatura, analisaremos a relação entre privacidade e liberdade, utilizando como base alguns dos trabalhos mais emblemáticos sobre o tema, como *Right to Privacy* (1890) de Samuel Warren e Louis Brandeis e *Privacy and Freedom* (1967) de Alan Westin. Então, na terceira seção, com maior destaque ao papel da tecnologia nesse processo evolucionário, voltaremos nossa atenção para o entendimento da privacidade como um bem coletivo, um direito fundamental.

O Capítulo 2, então, descreverá, à luz da contribuição de Shoshana Zuboff, como o capitalismo de vigilância surgiu em um momento de pouca regulação do espaço virtual e, aliado aos setores de inteligência do governo dos Estados Unidos, evoluiu de um plano de negócios do Google para criar um ambiente mundial de constante vigilância. Conforme mais empresas, como o Facebook, se inspiraram na iniciativa do Google e mais disseminado se tornou esse modelo econômico, a privacidade foi perdendo espaço no debate político e uma assimetria de poder em favor do setor privado evidenciou uma série de problemas sociais – os quais serão aprofundados no Capítulo 3.

Em menos de 20 anos de operação, o Google, pioneiro no capitalismo de vigilância, foi o principal responsável por definir as bases desse modelo econômico – uma vez que, devido à pressão dos investidores por maiores lucros, e pelo fato de que os líderes do Google eram contrários à ideia de um serviço pago, a empresa se voltou para um modelo de propaganda – e "(se)tornou a maior e mais bem-sucedida empresa de *big data* por ter o site mais visitado e, portanto, possuir a maior quantidade de *data exhaust*" (ZUBOFF, 2018, p. 24-5; 32).

Isto é, ao fazer uso dos "dados de usuários como matéria-prima para análise e produção de algoritmos" capazes de gerar publicidades "com precisão e sucesso cada vez maiores", as receitas do Google cresciam e "aumentava a motivação para uma coleta de dados cada vez mais abrangente. A nova ciência de análise de *big data* explodiu, impulsionada em grande parte pelo sucesso retumbante d[o] Google" (ZUBOFF, 2018, p. 32).

E uma das empresas a seguir um caminho muito semelhante foi o Facebook, que rapidamente se tornou uma empresa de publicidade, cuja principal atividade é

a vigilância. Isto é, como a empresa tem acesso ao identificador dos celulares de seus usuários, ela tem, portanto, conhecimento de "cada *site* que você visita, cada *link* que você segue." E assim, "o que você acaba vendo é determinado por algoritmos que filtram e direcionam esse conteúdo": mais do que seus interesses e amigos, o seu *feed* é determinado pelos interesses comerciais do Facebook. Com isso, "[o]s olhos dos usuários são sempre conduzidos para o ponto onde rendem mais para a empresa" (LANCHESTER, 2017).

O Capítulo 3, então, faz um mapeamento das consequências advindas da disseminação do capitalismo de vigilância e da operação de empresas como Google e Facebook, que sistematicamente violam a privacidade dos usuários e detêm demasiado controle sobre os dados pessoais dos usuários.

Na primeira seção, será discutido como o capitalismo de vigilância inaugura um novo tipo de biopoder que controla nossos corpos por meio de artefatos como a Internet das Coisas. Além disso, analisaremos como essas tecnologias tendem a perpetuar formas de discriminação e perpetuam *bias*. São exemplos desse cenário, práticas de *profiling* orientadas por dados demográficos, a editorialização algorítmica de *feeds* de notícias, modelos marcados por problemas de super e sub-representação, além da reprodução de machismos e do racismo.

Ademais, como o exemplo anterior do Facebook evidencia, a ideia de que se está interagindo com amigos se perde completamente – uma vez que esse processo é orientado por algoritmos e fórmulas comerciais – e, portanto, "(a) ideia que temos do que seja 'nós' vem ficando mais e mais estreita com o passar do tempo" (LANCHESTER, 2017), o que afeta gravemente a constituição de identidades.

Além disso, como será debatido na terceira seção, esse fenômeno abre cada vez mais espaço para a propagação de *fake news*, pois "o Facebook não tem qualquer interesse financeiro em só dizer a verdade. Isto é, "[p]ara o Facebook, que diferença faz se as notícias postadas são verdadeiras ou falsas? Seu interesse está no direcionamento dos anúncios, no *targeting*, e não no conteúdo que os acompanha" (LANCHESTER, 2017). Logo, dado o controle das *big tech* sobre os

sistemas de informação e a importância destes para a democracia, o principal modelo político do século XXI corre o risco de colapsar.

Por fim, no Capítulo 4, serão discutidas possíveis formas de resistência contra esse novo modelo econômico. Pelo lado do setor privado, algumas iniciativas têm sido tomadas para reduzir os danos político-sociais da tecnologia, como a implementação de princípios éticos no desenvolvimento de produtos e serviços. Ademais, alguns autores defendem que para viabilizar o exercício da resistência contra a *commodificação* desenfreada de informações pessoais, são necessários mecanismos de *accountability* ("prestação de contas"). Para Marc Rotenberg, privacidade é "sobre responsabilizar grandes atores governamentais e empresas privadas por suas decisões", "é um direito humano, particularmente na era digital, já que tanto sobre nós é baseado em nossos dados" (SHAW, 2017).

Em última instância, trata-se de resgatar a tecnologia e os mecanismos desenvolvidos pelo capitalismo de vigilância e utilizá-los a favor da humanidade. Giovanni Buttarelli, Supervisor Europeu de Proteção de Dados da União Europeia entre 2009-2014, defendia que a Inteligência Artificial deve ser parte da solução, não mais do problema. Advoga-se, portanto, pela necessidade de descentralizar a Internet e implementar mecanismos de governança, capazes de superar as assimetrias de poder presentes atualmente (ZICARI, 2019; ALMEIDA & DONEDA, 2016). Assim, conclui-se que é preciso um esforço coletivo, mas vindo principalmente da sociedade civil, que é o grupo mais afetado pelo capitalismo de vigilância e com a maior capacidade de mobilização.

CAPÍTULO 1

Privacidade: Conceitualização e Evolução Enquanto um Direito Fundamental

Fundamentado no conceito em inglês *privacy*, privacidade diz respeito ao resguardo de informações pessoais e da vida privada. Originalmente, esse princípio estava relacionado principalmente à propriedade e bens materiais, podendo ser entendido como um conceito tipicamente burguês. Contudo, ao longo do tempo, o escopo da privacidade evoluiu para incluir também aspectos mais íntimos do indivíduo, como suas ideias, pensamentos e crenças; em suma, informações pessoais.

Conforme tecnologias como a Internet e as redes sociais se tornam mais comuns ao cotidiano, o acesso e a distribuição de dados são facilitados e a privacidade é colocada em risco (MULHOLLAND, 2018). A título de exemplo, quando primeiro viralizou em 2019, o aplicativo de filtros faciais FaceApp se tornou uma grande preocupação em relação à privacidade após o senador norte-americano Chuck Schumer solicitar ao FBI que investigasse qual seria o uso dado às imagens coletadas e armazenadas pelos servidores da Wireless Lab, empresa dona do aplicativo. Na mesma época, no Brasil, o Procon tomou medidas legais contra o Google e a Apple – responsáveis pela distribuição do FaceApp no país –, multando-os em R$17,7 milhões após tomar conhecimento dos termos de uso definidos pela empresa quanto às finalidades dos dados coletados, que, no tópico "Conteúdo do Usuário", determina a concessão e "'o uso perpétuo, *irrevogável*, irrestrito e livre de royalties de todos os dados, que podem ser reproduzidos, modificados e distribuídos a outras empresas sem necessidade de permissão'" (LOPES, 2020, grifo meu).

No entanto, mesmo após o aplicativo reformular a política de privacidade especificando que "coleta e usa informações dos usuários", além de disponibilizar a possibilidade de exclusão das informações e anunciar que as fotos são "excluídas automaticamente entre 24h e 48h depois da última edição", especialistas recentemente demonstraram preocupação com possíveis usos secundários das

imagens. “[P]elo fato da tecnologia de reconhecimento facial que permite as edições na face ser uma ferramenta usada principalmente para a autenticação de senhas, o usuário deve ter bastante cuidado ao compartilhar sua imagem com terceiros.” E, uma vez que a empresa usa Inteligência Artificial para fazer as modificações faciais, esta poderia vender as fotos para empresas semelhantes (LOPES, 2020).

No entanto, mesmo que violações à privacidade como esta despertem sentimento de revolta ou medo, não podemos simplesmente classificá-las como algo “errado.” É preciso identificar os valores fundamentais que estão em risco quando questões de privacidade se mostram problemáticas para uma sociedade. “*The task is not to realize the true universal values of ‘privacy’ in every society. The law puts more limits on us than that: The law will not work as law unless it seems to people to embody the basic commitments of their society*” [1] (WHITMANT, 2004, p. 1220; SOLOVE, 2006).

Para Brunton e Nissenbaum (2015), privacidade é um conceito complexo e até mesmo contraditório: expresso em leis e políticas, tecnologias, filosofia, mas também conversas cotidianas. Para os autores, se abrirmos a “caixa de ferramentas” da privacidade, gaveta por gaveta, podemos encontrar “políticas e leis nos níveis local, nacional e global; tecnologias comprovadamente seguras, como criptografia; ações de divulgação e práticas de indivíduos; sistemas sociais de confidencialidade (por exemplo, de jornalistas, padres, médicos e advogados); e mais” (2015, p. 45-6, tradução minha[2]). Isto é, trata-se de um termo extremamente disseminado entre os mais diversos aspectos da vida em sociedade, incluindo desde o nível global por meio de normas e políticas, até questões mais básicas do cotidiano como a navegação em redes sociais.

---

[1] Tradução: A tarefa não é realizar os verdadeiros valores universais de "privacidade" em todas as sociedades. A lei nos impõe mais limites do que isso: a lei não funcionará como lei a menos que pareça às pessoas que incorpora os compromissos básicos de sua sociedade (WHITMANT, 2004, p. 1220).

[2] Original: “*If we open up privacy’s tool chest, drawer by metaphorical drawer, we find policy and law at the local, national, and global levels; provably secure technologies, such as cryptography; the disclosure actions and practices of individuals; social systems of confidentiality (for example, those of journalists, priests, doctors, and lawyers); steganographic systems; collective withholding and omerta on the part of a community; and more*” (BRUNTON & NISSENBAUM, 2015, p. 45-6).

Contudo, em se tratando de um termo tão versátil – no sentido de adaptável, aplicável a diversas situações –, é preciso levar em conta as consequências de possíveis perigos: em nome da segurança, a privacidade pode ser deturpada e em contextos como a Guerra ao Terror e as políticas antiterroristas da União Europeia, indiscriminadamente violada (BRUNTON & NISSENBAUM, 2015; FRIEDEWALD et al, 2017).

Além disso, é importante ressaltar o papel do Estado e dos desafios impostos pela vida em sociedade para melhor compreendermos como a noção de privacidade é manipulada. Enquanto autores como Hobbes, Locke e Rousseau têm uma visão mais individualista no que diz respeito à formulação do Estado – fazendo com que a separação entre público e privado tenda a colocar questões de "maior importância" no primeiro plano, e questões ligadas ao pessoal (como religião) no segundo –, autores como Bockenforde e Fischer veem a questão de outro modo. Focados em entender como sistemas políticos se autolegitimam e como "decisões coletivamente vinculativas" afetam a comunidade, ambos argumentam que a "formação do Estado liberal e seu objetivo real se baseia na necessidade de conter ameaças emanadas da religião" (FÜHRDING, 2013, p. 124-5, tradução minha [3]).

> *Fischer further explains how, throughout the following centuries, the notion that legitimate power depends on rightful legislation became prevalent. This is the task of the citizens. To put in a nutshell, the idea is that law is the highest authority, outranking even the sovereign. Furthermore, the idea of the commonweal is detached from spiritual conceptions of order and legitimized according to its function. This resulted not only in a 'secularization of political thinking' (2009:23) but also made contradicting opinions about the definition of the common good possible* (FÜHRDING, 2013, p. 126)[4].

[3] Original: "*Central to both Bockenforde's and Fischer's argument is the idea that the formation of the liberal state and its actual purpose is grounded in the need for containing threats emanating from religion—the result of contradictory religious truth claims (Fischer 2009: 50). These considerations are closely linked to the questions of how "collectively binding decisions" can be brought about in the commonwealth (Fischer 2009: 9) and how the political system legitimizes itself (Bockenforde 1976:42-43,57-61)*." (FÜHRDING, 2013, p. 125).

[4] Tradução: Fischer explica ainda como, ao longo dos séculos seguintes, prevaleceu a noção de que o poder legítimo depende da legislação correta. Essa é a tarefa dos cidadãos. Resumindo, a ideia é que a lei é a autoridade máxima, superando até mesmo o soberano. Além disso, a ideia de bem comum é separada das concepções espirituais de ordem e legitimada de acordo com sua função. Isso resultou não apenas em uma "secularização do pensamento político" (2009: 23), mas também tornou possíveis opiniões contraditórias sobre a definição do bem comum (FÜHRDING, 2013, p. 126).

Nesse sentido, torna-se fácil entender o motivo da ausência de uma definição universal de privacidade. Isto é, a partir da contribuição de Fischer, podemos perceber como há uma dificuldade de se chegar a um consenso sobre assuntos que dizem respeito a uma coletividade.

Para Doneda (2006), então, "a tutela da privacidade é melhor enquadrada dentro do que foi descrito por Pietro Perlingieri como uma situação subjetiva complexa", expressa não por meio do exercício arbitrário do poder pelo seu titular, mas "em um complexo de interesses, tanto do titular quanto da coletividade, que pode dar origem a poderes bem como a deveres, obrigações, ônus aos envolvidos" (DONEDA, 2006, p. 101).

Isto posto, o objetivo deste capítulo é fazer uma breve contextualização do conceito de privacidade por meio de uma revisão de literatura de modo a entender como este evoluiu ao longo do tempo, até ser entendido atualmente como um direito fundamental e, que, como tal, deve ser protegido e garantido pelo Estado. Assim, num primeiro momento, valendo-nos principalmente das contribuições de John Locke e James Madison, analisaremos como a privacidade foi a princípio conceitualizada na lei norte-americana como uma forma de proteção da propriedade dos indivíduos. E, por serem categorias bastante próximas na literatura, analisaremos o papel da liberdade no entendimento de privacidade, discutindo a contribuição de alguns dos trabalhos mais emblemáticos sobre o tema, como *Right to Privacy* (1890) de Samuel Warren e Louis Brandeis e *Privacy and Freedom* (1967) de Alan Westin. Por fim, dando especial atenção para o papel da tecnologia nesse processo evolucionário, voltaremos nossa atenção para o entendimento da privacidade como um bem coletivo, um direito fundamental.

1.1 Privacidade como Propriedade

Em sua origem, a noção de privacidade segundo Westin (1967) pode ser relacionada a sociedades primitivas e ao reino animal. Em sua obra *Privacy and Freedom*, o autor bebe de estudos antropológicos de forma a compreender a evolução do conceito na modernidade e conclui que privacidade é a "reivindicação

de indivíduos, grupos ou instituições para determinar por si próprios quando, como e em que medida as informações sobre eles são comunicadas a terceiros" (WESTIN, 1967, p. 24-5, tradução minha[5]).

Ao comparar, então, o comportamento humano ao de animais, é possível observar uma série de semelhanças, em especial, quanto à reclusão. Westin descreve como todos os mamíferos têm momentos de vivência em grupo e de isolamento físico-social dos demais da espécie, sendo o equilíbrio entre esses um dos mais básicos processos da vida animal. Dessa forma, uma das heranças do mundo animal, os sentidos físicos (visão, olfato, audição, toque e paladar) são os principais medidores para o entendimento humano de distanciamento: "*What is considered 'too close' a contact and therefore an 'invasion of privacy' in human society will often be an odor, a noise, a visual intrusion, or a touch; the mechanism for defining privacy in these situations is sensory*" [6] (WESTIN, 1967, p. 26).

É possível identificar, portanto, que, num primeiro momento, a privacidade tem um forte caráter individualista, expressando "a feição do direito a ser deixado só", mas também traços tipicamente burgueses, elitistas. Segundo Doneda (2006), "[a] este período remonta o paradigma da privacidade como uma *zero-relationship*: a ausência de comunicação entre um sujeito e os demais" (DONEDA, 2006, p. 7).

Por outro lado, segundo Cloud (2018), liberdade e o que hoje entendemos como direitos de privacidade são definidos pela Quarta Emenda à Constituição dos Estados Unidos em termos de personalidade ("*personhood*") e propriedade porque à época o termo "privacidade" não fazia parte do vocabulário político. Assim sendo, sofrendo influência de filósofos como John Locke, direitos de liberdade e privacidade eram entendidos em termos de direitos de propriedade, "o principal

[5] Original: "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (WESTIN, 1967, p. 24).

[6] Tradução: O que é considerado um contato "muito próximo" e, portanto, uma "invasão de privacidade" na sociedade humana, muitas vezes será um odor, um ruído, uma intrusão visual ou um toque; o mecanismo para definir privacidade nessas situações é sensorial (WESTIN, 1967, p. 26).

baluarte contra invasões impróprias do governo na vida das pessoas" (CLOUD, 2018, p. 42-3, tradução minha[7]).

Especificamente, a Emenda protege "casas", mas também "papéis" e "efeitos." Dessa forma, aquilo que estiver sob a posse de um indivíduo em sua casa – ou espaços que venha a ocupar, como escritórios ou quartos de hotel – deve ser protegido contra procuras indevidas. Estão proibidas também, portanto, invasões aos locais onde os objetos pessoais do indivíduo estejam guardados (CLOUD, 2018, p. 40-1).

Na segunda metade do século XVIII e durante a Revolução Americana, teorias baseadas na ideia de propriedade tiveram uma forte influência sobre o pensamento político-democrático nos Estados Unidos e na Inglaterra. E o *Segundo tratado sobre o governo* (1689) de Locke foi certamente um dos textos mais importantes para a consolidação dessa ideologia, pois, segundo o autor, a propriedade de uma pessoa estava além dos objetos que possuía, englobando também seus direitos (CLOUD, 2018, p. 44, 47).

Ao definir a propriedade de um homem, portanto, enquanto sua "vida, trabalho e seus produtos", quando estes incluem objetos externos, também são transformados em parte de sua propriedade pois são extensões de seu ser, expressões de sua própria personalidade. Consequentemente, muitas vezes conquistados a um alto custo, os direitos "eram propriedades possuídas por pessoas tão seguramente quanto suas propriedades físicas e protegidas contra violações tanto quanto qualquer invasão física em terra ou contra a posse de bens pessoais" (CLOUD, 2018, p. 45-6, tradução minha[8]).

De forma semelhante, James Madison em seu ensaio *Property* (1792), dá um passo além de Locke e afirma que as ideias, habilidades, crenças e a possibilidade de exercê-las são a propriedade mais cara de um homem. Assim, antes mesmo da emergência do direito legal à privacidade, "*common law judges*" já reconheciam que o autor de quaisquer escritos (ou outras formas de expressão

[7] Original: "*Property stood as a primary bulwark against improper government intrusions into the lives of the people*" (CLOUD, 2018, p. 42-3).
[8] Original: "*Rights, often won at great cost, were property possessed by people as surely as their physical property and secured against violation as much as any physical trespass onto land or against possession of personal property*" (CLOUD, 2018, p. 45).

criativa) deveria ter seu conteúdo protegido por serem documentos privados que este criara, incluindo o poder de determinar quem pudesse usar desta propriedade privada e para quais propósitos (CLOUD, 2018, p. 48-9, 56).

Aqui é possível perceber os vasos comunicantes entre propriedade e liberdade; uma vez que, para Madison, é dever do governo garantir a proteção dessa propriedade, cujos elementos mais importantes não são objetos tangíveis, mas as opiniões – assim como a liberdade de formulá-las e expressá-las –, os direitos e pensamentos do indivíduo. Nesse sentido, "*[t]his broad theory of property 'was intimately related to the development of the human personality, to the exercise of independent thought and creative powers*'" [9] (CLOUD, 2018, p. 48-50).

1.2 Privacidade como Liberdade

Por outro lado, a lei de privacidade alemã, definida mais tardiamente, diz respeito à questão de "personalidade", um conceito muito particular à filosofia alemã e conectado à noção de "liberdade de ser", cujas origens remontam à proteção contra insulto (ideia derivada da filosofia romana), mas também à noção de "direito do criador" (direito autoral) (WHITMANT, 2004).

Diferente da ideia norte-americana de "*freedom*" como oposta à tirania, os pensadores alemães do século XIX tendem a pensar "*freedom*" como contrária ao determinismo. Isto é, inspirados nas ideias de Kant e Hegel, os alemães entendem que a liberdade dos indivíduos estaria ligada à possibilidade de cada um realizar por completo seu potencial, expressando suas capacidades e poderes, suas particularidades, e, portanto, sua personalidade. Nesse sentido, foi desenvolvida uma tradição legal que entende a privacidade como parte da "livre autorrealização" dos indivíduos, oferecendo proteção à personalidade de cada um (WHITMANT, 2004, p. 1181-2).

Como consequência, a lei alemã dá importância especialmente para o "direito do criador" como forma de proteger a individualidade deste, assim como

[9] Tradução: Esta ampla teoria da propriedade 'estava intimamente relacionada ao desenvolvimento da personalidade humana, ao exercício do pensamento independente e dos poderes criativos' (CLOUD, 2018, p. 49-50).

de sua obra como parte de sua propriedade. Uma inovação do século XIX, a proteção dos direitos criativos do artista constitui para Whitmant (2004) um exemplo clássico da nova sensibilidade moderna a interesses imateriais. Parcialmente, então, trata-se de direitos autorais, mas também da expansão do controle do uso de um trabalho artístico – parte de sua propriedade –, protegendo a reputação do autor e garantindo sua liberdade de expressão, de sua personalidade (WHITMANT, 2004, p. 1184-5).

No clássico *Right to Privacy* (1890) – considerado por muitos um dos pilares para a definição norte-americana de privacidade – Samuel Warren e Louis Brandeis descrevem como a evolução da proteção do indivíduo sofreu mudanças ao longo do tempo: conforme mudanças políticas, econômicas e socias implicam no reconhecimento de novos direitos, são necessárias novas leis de proteção ao indivíduo. Em seus primeiros estágios, a lei somente oferecia proteção contra interferências físicas sobre o corpo e a propriedade. Mais tarde, veio a incorporar posses tangíveis e intangíveis do indivíduo. Liberdade significava estar livre de alguma restrição real, e no decorrer do tempo esta ideia foi ampliada englobando o direito de o indivíduo expressar suas opiniões religiosas, emocionais e intelectuais (WARREN & BRANDEIS, 1890, p. 193-4).

No entanto, conforme novas tecnologias de comunicação – como fotografias e jornais – se popularizavam, novas questões ligadas à proteção do indivíduo surgiam, como circulação não autorizada de retratos e a disseminação de artigos de fofoca que divulgam informações pessoais, tomando proporções nunca antes vistas e se mostrando completamente desrespeitosas à decência e moralidade (WARREN & BRANDEIS, 1890, p. 196).

Vale ressaltar, porém que, ao estudar as dinâmicas antropológicas presentes no entendimento moderno sobre privacidade, Westin (1967) defende que o elemento da curiosidade sobre a vida de outros não é uma característica exclusiva da modernidade, estando presente em “todas as sociedades primitivas”, sendo a fofoca uma maneira de conseguir informação pessoal detectada em todas as sociedades.

> *People want to know what others are doing, especially the great and the powerful, partly as a means of gauging their own performances and desires and partly as a means of vicarious experience, for by satisfying*

> *curiosity the individual experiences a sense of pleasure from knowing about exciting or awesome behavior in others* (WESTIN, 1967, p. 32)[10].

Como consequência, surge um novo mercado no qual o indivíduo cuja vida é exposta na mídia sofre não só invasões de sua privacidade, bem como "dores e angústias mentais, muito maiores do que poderiam ser infligidas por mera lesão corporal." Ademais, em se tratando de um comércio, a oferta cria demanda e, então, cada fofoca publicada alimenta a próxima, resultando no "rebaixamento de padrões sociais e da moralidade" (WARREN & BRANDEIS, 1890, p. 196, tradução minha[11]).

Portanto, Warren e Brandeis, assim como Westin, argumentam que ninguém tem o direito de publicar algo pessoal sobre outra pessoa sem o seu consentimento: somente o próprio indivíduo é capaz de determinar se algo sobre si pode ser revelado ao público, salvo quando este material é deliberadamente compartilhado com o público – isto é, publicado (WARREN & BRANDEIS, 1890, p. 198-9; WESTIN, 1967).

> *These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. (...) The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality* (WARREN & BRANDEIS, 1890, p. 205)[12].

No entanto, ao analisar a contribuição de Warren e Brandeis, Whitmant (2004) conclui que esta foi uma tentativa falha, segundo o autor, de transplantar

---

[10] Tradução: As pessoas querem saber o que os outros estão fazendo, especialmente os grandes e poderosos, em parte como um meio de avaliar seus próprios desempenhos e desejos e em parte como um meio de experiência indireta, pois, ao satisfazer a curiosidade, o indivíduo experimenta uma sensação de prazer em saber sobre comportamentos emocionantes ou incríveis em outros (WESTIN, 1967, p. 32).

[11] Original: "*but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury. (...) Each crop of unseemly gossip, thus harvested, becomes the seed of more, and, in direct proportion to its circulation, results in a lowering of social standards and of morality*" (WARREN & BRANDEIS, 1890, p. 196).

[12] Tradução: Essas considerações levam à conclusão de que a proteção conferida aos pensamentos, sentimentos e emoções, expressos por meio da escrita ou das artes, na medida em que consiste em impedir a publicação, é apenas uma instância da aplicação do direito mais geral do indivíduo para ser deixado sozinho. (...) O princípio que protege os escritos pessoais e todas as outras produções pessoais, não contra roubo e apropriação física, mas contra a publicação em qualquer forma, é na realidade não o princípio da propriedade privada, mas o de uma personalidade inviolável (WARREN & BRANDEIS, 1890, p. 205).

noções europeias de privacidade para os Estados Unidos. Isto é, o autor defende que na Europa a ideia de proteger a dignidade do indivíduo (nomeada pelos americanos de "*right to be let alone*") é amplamente difundida há séculos, enquanto nos Estados Unidos, esse princípio não se consolidou como Warren e Brandeis esperavam (WHITMANT, 2004).

O autor argumenta que as várias leis de proteção às minorias presentes hoje na Europa – direitos trabalhistas, das mulheres, de prisioneiros etc. – não se devem aos horrores do nazifascismo, como muitos defendem. Na verdade, leis são respostas aos séculos de desigualdades perpetuadas no continente, trata-se do resultado de séculos de revolta contra sistemas de privilégio (WHITMANT, 2004, p. 1166).

Segundo Whitmant (2004), existem, nos dois lados do Atlântico, diferentes entendimentos culturais, que produziram distintas leis e culturas de privacidade. Na Europa, valores de proteção da honra e da imagem do indivíduo, assim como de igual tratamento são mais valorizados. Dessa forma, a ideia de privacidade inclui não só o direito de controlar como informações pessoais – a citar, dados de consumo – são manipuladas, mas também o direito de prisão justa (caso seja necessário) e o direito de privacidade no ambiente de trabalho. Por outro lado, nos Estados Unidos, valores de liberdade tendem a ser os norteados da sociedade, em especial, liberdade contra o Estado. "*At its conceptual core, the American right to privacy still takes much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home*" [13] (WHITMANT, 2004, p. 1160-71).

Aqui, podemos observar novamente as fortes interseções entre as noções de liberdade e propriedade, pois, assim como Cloud (2018), Whitmant identifica a origem legal da ideia de privacidade na Quarta Emenda da Constituição dos Estados Unidos, quando se entende por privacidade o direito de proteção contra buscas ilegítimas. Com o tempo, esse entendimento amadureceu como um direito mais

[13] Tradução: Em seu núcleo conceitual, o direito americano à privacidade ainda assume grande parte da forma que assumiu no século XVIII: é o direito à liberdade de intrusões pelo Estado, especialmente em sua própria casa (WHITMANT, 2004, p. 1161).

abrangente que proíbe a intromissão do Estado na vida dos cidadãos (CLOUD, 2018; WHITMANT, 2004, p. 1211-2).

> (…) *American "privacy" law, however ingenious its elaborations, always tends to imagine the home as the primary defense, and the state as the primary enemy. This gives American privacy law a distinctive coloration. Where American law perceives a threat to privacy, it is typically precisely because the state has become involved in the transaction* (WHITMANT, 2004, p. 1215)[14].

Uma vez que no Novo Mundo a casa é entendida como "uma cidadela de soberania individual" (WHITMANT, 2004, p. 1161-2, tradução minha[15]), o indivíduo tem sua privacidade garantida quando está livre da interferência do Estado em sua vida pessoal, o que deveria ser suficiente para exercer sua liberdade.

De forma semelhante, John Stuart Mill (2001) argumenta que a conduta do indivíduo só diz respeito à sociedade em assuntos de matéria coletiva, que têm relação com outros. "Na parte que apenas se preocupa, sua independência é, por direito, absoluta. Sobre si mesmo, sobre seu próprio corpo e mente, o indivíduo é soberano" (MILL, 2001, p. 13, tradução minha[16]).

Para Westin (1967), no entanto, é importante reconhecermos a dimensão social ligada à curiosidade e vigilância, pois, como todas as sociedades humanas criam normas de convivência, é preciso que haja mecanismos que as façam cumprir, investigando transgressões, observando comportamento e criando imaginários de "culpa." Nesse sentido, de forma a manter a unidade social e garantir direitos individuais, tais mecanismos de vigilância e punição são "aceitos" pela sociedade, reforçando regras e tabus sociais (WESTIN, 1967, p. 32-3).

Já Mill entende que, liberdade diz respeito à perseguição do nosso próprio bem de maneira irrestrita, desde que não coloquemos impedimentos para que os outros façam o mesmo ou tentemos privá-los desse direito. Ao invés de tentar impor

---

[14] Tradução: A lei de "privacidade" americana, por mais engenhosa que seja sua elaboração, sempre tende a imaginar o lar como a principal defesa e o Estado como o principal inimigo. Isso dá à lei de privacidade americana uma coloração distinta. Onde a lei americana percebe uma ameaça à privacidade, normalmente é exatamente porque o Estado se envolveu na transação (WHITMANT, 2004, p. 1215).

[15] Original: "*a New World in which it seems fundamentally important to preserve the home as a citadel of individual sovereignty*" (WHITMANT, 2004, p. 1162).

[16] Original: "*In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign*" (MILL, 2001, p. 13).

um único estilo de vida a todos, a sociedade se beneficia mais ao deixar que os indivíduos ajam livremente, pois "cada um é o guardião adequado de sua própria saúde, seja corporal, mental ou espiritual" (MILL, 2001, p. 16, tradução minha[17]).

De maneira semelhante, Julie Cohen (2000) contesta a ligação frequentemente defendida entre privacidade e propriedade argumentando que isto poderia fazer da privacidade um bem comercializável ("*a marketable commodity*"). Assim, a autora defende que a privacidade deve ser entendida como um valor tal qual igualdade ou liberdade, uma vez que esta é essencial para o desenvolvimento de autonomia moral e independência de pensamento. Um certo grau de liberdade do julgamento por terceiros, então, tem propósitos vitais nos níveis individual e coletivo, pois sem o espaço proporcionado pela privacidade para o indivíduo trabalhar na construção do *self*, suas crenças e desejos têm mais probabilidade de se enquadrarem no espectro limitado do *mainstream* (COHEN, 2000, p. 1423-4).

Em suma, a vida em sociedade torna necessária a existência de privacidade, pois, ao participar de atividades coletivas, governos, indivíduos e instituições podem impor consequências negativas sobre os demais. Portanto, a privacidade permite que as pessoas interajam entre si eliminando barreiras e impeditivos sociais; "*Privacy is the relief from a range of kinds of social friction*" [18] (SOLOVE, 2006, p. 484).

1.3 Privacidade como Bem Coletivo

Segundo Mulholland (2018), "a ampliação do conceito de *privacy* se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais." À medida que tecnologias como a Internet e a biotecnologia se desenvolveram, "o acesso a dados sensíveis e, consequentemente, a sua divulgação, foram facilitados de forma extrema." Assim, o acesso indevido por terceiros a dados pessoais é facilitado e, consequentemente, surgem novas possibilidades de violação da vida privada. "Com isso, a tutela da privacidade passa a ser vista não só como o

[17] Original: "*Each is the proper guardian of his own health, whether bodily, or mental and spiritual*" (MILL, 2001, p. 16).
[18] Tradução: A privacidade é a rendição de uma série de tipos de atrito social (SOLOVE, 2006, p. 484).

direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada" (MULHOLLAND, 2018, p. 172).

Isto é, conforme cada vez mais interagimos com mídias digitais e mais processos e relações são desenvolvidos no meio digital, mais dados e informações pessoais são compartilhados virtualmente, o que implica em consequências sobre a forma como interagimos com outras pessoas, mas também com nós mesmos – sobre nossa personalidade.

E o momento que vivemos atualmente em que boa parte da população está há meses em isolamento social devido à pandemia de Covid-19 é extremamente simbólico desse fenômeno. Além de amplificar atividades cada vez mais executadas por intermédio de computadores e *smartphones* como fazer compras, estudar e trabalhar, esse momento trás importantes inovações de cunho social, pois a convivência coletiva passa a ser mediada pela Internet como nunca antes. Para alguns, a casa virou academia, sala de aula, escritório, área de lazer, consultório médico e até igreja conforme diversos aspectos da vida social passam a ser realizados virtualmente. Todas essas atividades, então, expressam algo sobre nós como indivíduos, e também como usuários.

Nesse processo, nossa privacidade é constantemente violada à medida que nossas ações são vigiadas por algumas (poucas) empresas que, em busca de lucro, usam os dados dos usuários da maneira que julgam melhor. Vejamos o caso da Zoom, uma plataforma de videochamadas que registrou aumento explosivo de número de usuários logo após o início da implementação de medidas de isolamento social ao redor do mundo, e, ao mesmo tempo, é alvo de diversos debates a cerca de cibersegurança.

Sem antecipar que se tornaria tão popular, a empresa não tomou as medidas de segurança necessárias em relação à privacidade, recebendo críticas por "enviar dados dos usuários para o Facebook, alegar falsamente que o aplicativo tinha criptografia de ponta a ponta e permitir que os *hosts* da reunião rastreassem os participantes", além de deixar usuários de computadores Mac vulneráveis à intercepção de câmeras e microfones, e permitir que convidados entrassem em reuniões sem serem convidados, acessando os *links* por meio de publicações em

redes sociais ou mesmo "adivinhando o código de nove dígitos" (WAKEFIELD, 2020, tradução minha[19]).

Dessa forma, há uma necessidade emergente de controle sobre o espaço virtual pois os antigos entendimentos de que o indivíduo é quem tem autoridade para definir como e para quem seus dados são disponibilizados – como visto anteriormente por meio das contribuições de Warren e Brandeis (1890) e Westin (1967) – não mais se aplicam no século XXI.

Segundo Zuboff (2019), conforme os direitos decisórios sobre privacidade são apropriados pelas *big techs*, a privacidade é redistribuída: o poder de decidir como e o que as pessoas compartilham sobre si não está em suas mãos, mas concentrado nas empresas que dominam a Internet (ZUBOFF, 2019, p. 90-1).

> Considerando que se caminha cada vez mais e com maior intensidade para uma sociedade governada por dados, o ambiente social no qual se concretiza a ideia de privacidade informacional passa a ser qualificado pela proteção dos direitos da pessoa de manter o controle sobre seus dados, por meio de sua autodeterminação informativa (liberdade), visando a não discriminação (igualdade). Portanto, o problema da privacidade hoje é causado pelo conflito consequente da assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados. Esta assimetria gera um desequilíbrio social que, por sua vez, leva à violação dos princípios da igualdade e da liberdade. Proteger de maneira rigorosa os dados pessoais sensíveis se torna, assim, instrumento para a efetivação da igualdade e da liberdade (MULHOLLAND, 2018, p. 176-7).

Nesse sentido, a proteção de dados está intimamente ligada ao "livre desenvolvimento da personalidade", podendo ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio" (RODOTÀ, 2008, p. 14). Isto é, se cada vez mais, as relações sociais se dão por intermédio da tecnologia, mais esta tem poder sobre nosso comportamento. Como Zuboff alerta, a assimetria de poder entre os indivíduos e as empresas que dominam o espaço virtual cresce num ritmo tal que corremos o risco de perder nossa individualidade e nos tornarmos uma nação de zumbis sem qualquer tipo de controle sobre nosso comportamento ou capacidade decisória, devido à alienação da população desse

[19] Original: "*Zoom has been criticised for a range of privacy issues, including sending user data to Facebook, wrongly claiming the app had end-to-end encryption, and allowing meeting hosts to track attendees*" (WAKEFIELD, 2020).

processo, mas também à ineficiência dos sistemas regulatórios sobre esse setor do capitalismo (ZUBOFF, 2019).

No processo evolutivo da privacidade, então, conforme novas preocupações surgem, há uma "'força expansiva' da proteção de dados pessoais", "mais que uma mera característica congênita dos chamados 'novos direitos'": há uma "mutação do ambiente no qual circulam os dados", surgindo novos atores e preocupações ligados à garantia da liberdade de expressão. Pois, já que se corre o risco de haver uma conformação de comportamento generalizada, a sociedade pode perder sua característica mais básica, a diversidade de pensamento. E, portanto, "[h]oje, a privacidade passa a apresentar também uma dimensão coletiva" (DONEDA, 2006, p. 17-20; ZUBOFF, 2019).

> Desta dimensão coletiva surge, enfim, a conotação contemporânea da proteção da privacidade, que manifesta-se sobretudo (porém não somente) através da proteção de dados pessoais; e que deixa de dar vazão somente a um imperativo de ordem individualista, mas passa a ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que na disciplina da privacidade passe a se definir todo um estatuto que perpassa as relações da própria personalidade com o mundo exterior (DONEDA, 2006, p. 21).

De maneira semelhante, Regan (1995) argumenta que ao garantir a privacidade no nível individual, o coletivo é quem na verdade mais se beneficia. A autora entende que a privacidade deve ser vista cada vez mais como um bem comum, pois frequentemente pensa-se no indivíduo quando pensamos no papel da privacidade sobre a promoção de valores como desenvolvimento humano, liberdade de pensamento e ação, e autonomia. No entanto, ao fazê-lo, não damos a devida atenção para a importância desses valores para o desenvolvimento de sociedades liberais, que estão baseadas em princípios como liberdade de associação, religião e expressão (REGAN, 1995; NISSENBAUM, 2010, p. 86).

CAPÍTULO 2

A *Assemblagem* da Vigilância e a Captura do Comportamento Humano

O ano de 2001 foi marcado por uma série de mudanças que afetariam a economia e a forma como nos relacionamos, definindo importantes distinções do século XX e ditando as novas regras sociais desse novo momento histórico. Os ataques terroristas ocorridos em 11 de setembro nos Estados Unidos são um desses fenômenos capazes de definir um "passado" e um "futuro" e que impactam fortemente a constituição de uma estrutura social. Conforme o governo dos Estados Unidos – e boa parte dos países ocidentais – responde aos ataques com a expansão e a centralização de mecanismos de vigilância em prol da segurança, David Lyon (2001), sociólogo e coordenador do Surveillance Studies Centre da Queen's University (Kingston, Canadá), argumenta que há uma maior tendência de depender de novas tecnologias, e tais práticas influenciam a forma como vivemos em sociedade (LYON, 2001).

Naquele primeiro momento, a principal preocupação era a segurança, e discussões de privacidade foram rapidamente deixadas de lado. Medidas como o *Patriot Act* e o *Terrorist Screening Program* nos Estados Unidos, assim como a expansão de poderes de inteligência e agências de *law-enforcement* na Europa promoveram um aumento dramático da coleta "sem mandato" de informações pessoais. Nesse sentido, a "guerra ao terror" é caracterizada por um "estado de exceção" capaz de legitimar tais buscas em nome da segurança (ZUBOFF, 2019, p. 112-5).

Inspirado nos trabalhos de Gilles Deleuze e Felix Guattari (1987), Lyon defende que a partir de então os mecanismos de vigilância tendem menos a criar uma figura centralizadora pela qual as atividades e atitudes individuais perpassam,

mas a dispersar tais práticas em meio ao cotidiano, formando uma espécie de "assemblagem[1] de vigilância" onde a percepção da vigilância é menos evidente.

> *In the assemblage, surveillance works by abstracting bodies from places, splitting them into flows to be reassembled as virtual data-doubles, calling in question once again hierarchies and centralized power. One important aspect of this is that the flows of personal and group data percolate through systems that once were much less porous; much more discrete and watertight. Thus, following September 11, surveillance data from a myriad of sources - supermarkets, motels, traffic control points, credit card transaction records and so on - were used to trace the activities of the 'terrorists' in the days and hours before their attacks. The use of searchable databases makes it possible to use commercial records previously unavailable to police and intelligence services and thus draws on all manner of apparently "innocent" traces* (LYON, 2001)[2].

Para viabilizar tal projeto, o governo norte-americano se aliou a empresas de tecnologia emergentes, que viram no 11 de setembro o momento perfeito para pôr em prática novos produtos e técnicas (LYON, 2001). E segundo Zuboff (2019), um dos maiores beneficiados por esse momento de estado de exceção foi o Google, cujas capacidades tecnológicas foram cruciais para o desenvolvimento dos novos sistemas de vigilância instaurados em meio à guerra ao terror (ZUBOFF, 2019, p. 113-5).

Até então, o governo estadunidense se esforçava para entender como regular as novas empresas de tecnologia, uma vez que o espaço virtual ainda era pouco conhecido pelos órgãos legislativos. No entanto, a partir de 2001, os interesses do governo mudam drasticamente, fortalecendo uma grande afinidade entre

---

[1] O conceito de "*assemblage*" foi incorporado aos estudos de vigilância como uma maneira de identificar a presença da vigilância nos mais variados aspectos de nossas vidas, como o uso de redes sociais, troca de *e-mails* e caminhar em *shoppings* e espaços públicos monitorados por câmeras. Segundo John Gilliom e Torin Monahan (2013), esse fenômeno "remove indivíduos e práticas do contexto social, traduzindo-os em 'dados' que podem ser analisados de forma discreta, trocados livremente e recombinados para fornecer uma representação aparentemente objetiva (...) dos indivíduos." Portanto, não há uma única força central que nos monitora: a vigilância é constante e praticada por uma série de atores em diversas situações (GILLIOM & MONAHAN, 2013, p. 22, tradução minha).

[2] Tradução: Na assemblagem, a vigilância funciona abstraindo corpos de lugares, dividindo-os em fluxos a serem remontados como dublês de dados virtuais, questionando novamente as hierarquias e o poder centralizado. Um aspecto importante disso é que os fluxos de dados pessoais e de grupo percolam sistemas que antes eram muito menos porosos; muito mais discretos e à prova de dúvidas. Assim, após 11 de setembro, dados de vigilância de uma miríade de fontes - supermercados, motéis, pontos de controle de tráfego, registros de transações de cartão de crédito e assim por diante - foram usados para rastrear as atividades dos "terroristas" nos dias e horas antes de seus ataques. O uso de bancos de dados pesquisáveis possibilita o uso de registros comerciais anteriormente indisponíveis para a polícia e os serviços de inteligência e, portanto, utiliza todos os tipos de vestígios aparentemente "inocentes" (LYON, 2001).

Washington e o Vale do Silício: dado o caráter emergencial da situação e a vontade do Google de se consolidar no mercado, é criada uma "deformidade histórica sem igual" – o "excepcionalismo de vigilância" ("*surveillance exceptionalism*"), que naturaliza e legitima a vigilância e a invasão da privacidade individual (ZUBOFF, 2019, p. 115, tradução minha).

Nesse sentido, o objetivo, incluído no contrato de US$2.07 milhões entre as agências de segurança e o Google, era beneficiar o governo com as capacidades tecnológicas cada vez mais avançadas do Google enquanto este desenvolve e comercializa mecanismos de vigilância e segurança difusos. Assim, *"[s]urveillance exceptionalism helped to shape the evolutionary course of information capitalism by creating an environment in which Google's budding surveillance practices were coveted rather than contested*" [3](ZUBOFF, 2019, p. 117;120).

Ademais, durante esse período ocorreu a chamada "Crise das ponto com." Devido ao aumento do interesse pelas novas empresas de tecnologia, houve, nessa época, uma supervalorização destas – algumas chegando a ser avaliadas em bilhões de dólares. E mesmo após o presidente do Sistema de Reserva Federal, de 1987 a 2006, Alan Greenspan alertar para uma "exuberância irracional" dos preços, "o frenesi de investimentos continuou - até que a bolha estourou, quando ficou claro que muitas dessas empresas não eram rentáveis." Com isso, em outubro de 2002, uma queda drástica do índice Nasdaq provocou "uma recessão nos Estados Unidos com reflexos globais", o que motivou essas empresas a mudarem seus planos de negócios (BARRÍA, 2017).

Assim, além dos registros pessoais serem cada vez mais usados por entidades governamentais, os dados também passaram a ser economicamente explorados pelas empresas que os detêm. De forma a responder à bolha financeira e encontrar uma fonte mais segura e estável de receita, as empresas como Google foram pressionadas a redefinir a maneira como conduziriam seus negócios e uma das soluções encontradas foi a abertura de leilões para propagandas em seus *sites*. Conforme usavam esse mecanismo, as empresas foram percebendo que poderiam usar os registros de busca dos usuários e demais dados pessoais, como endereço de

[3] Tradução: O excepcionalismo da vigilância ajudou a moldar o curso evolutivo do capitalismo da informação ao criar um ambiente no qual as práticas de vigilância do Google eram mais cobiçadas do que contestadas (ZUBOFF, 2019, p. 117).

IP. Viram que poderiam direcionar os anúncios de forma cada vez mais precisa e, assim, poderiam cobrar mais pelos serviços de propaganda, pois haveria uma maior probabilidade de o indivíduo de fato clicar na mensagem (ZUBOFF, 2019, p. 73-8).

Isto é, conforme a parceria entre os setores público e privado em nome da segurança e ao redor da vigilância se fortalecia, uma espécie de padrão surgia. Dados os benefícios dessa relação – os quais serão discutidos mais a fundo ao longo do capítulo –, a coleta de informações pessoais por parte do governo, mas também por empresas privadas, se torna tão atrativa que deixar de fazê-la se torna muito oneroso (ZUBOFF, 2019, p. 121).

Consequentemente, nesse novo modo de fazer negócios, a privacidade é constantemente violada em nome do lucro. E, devido aos novos esforços de segurança, a recém-formada parceria entre governo e empresas precisava ser protegida, mesmo que isso significasse o desrespeito dos direitos individuais dos usuários.

Portanto, ao longo do século XXI, conforme mais objetos são conectados à Internet e mais aspectos do cotidiano são mediados por esses, a "assemblagem de vigilância" é naturalizada e cada vez mais estamos alienados desse processo. O presente capítulo, então, se propõe a detalhar como se dá esse processo de apropriação dos dados pessoais por empresas de tecnologia, em especial, pelo Google e Facebook; para que em seguida sejam discutidas suas consequências para a vida em sociedades democráticas. Assim, nas próximas seções, discutiremos os principais elementos do que Shoshana Zuboff classifica como "capitalismo de vigilância" por meio dos casos do Google e Facebook, os principais responsáveis pela disseminação desse novo modelo econômico baseado na coleta de dados pessoais.

2.1 Fundamentos do Capitalismo de Vigilância

As inovações tecnológicas do *iPod* e *iTunes* proporcionaram a portabilidade da música, revolucionando a relação entre consumidor e música. Ao eliminar os CDs, os custos com produção, armazenamento e transporte foram eliminados. Além

disso, a digitalização das músicas permitiu que os usuários personalizassem seus aparelhos da maneira que desejassem a qualquer momento adicionando ou excluindo o que quisessem, o que trouxe consequências financeiras para a indústria da música, mas atendeu perfeitamente os desejos dos consumidores. "*Just as Ford tapped into a new mass consumption, Apple was among the first to experience explosive commercial success by tapping into a new society of individuals and their demand for individualized consumption*"[4] (ZUBOFF, 2019, p. 29-30).

Essa mudança de consumo se deve em grande parte, segundo Zuboff, ao embate destrutivo entre a mudança centenária do coletivo para o indivíduo e a implementação da lógica econômica neoliberal, caracterizada pelo objetivo de "reverter, subjugar, impedir e até mesmo destruir o impulso individual de autodeterminação psicológica e agência moral" (ZUBOFF, 2019, p. 30-1, tradução minha[5]).

Isto é, ao considerar, que o "capitalismo evolui de acordo com as necessidades das pessoas em um determinado tempo e espaço", as inovações da Apple são uma expressão de uma "segunda modernidade", que surge a partir da segunda metade do século XX, período marcado pela emergência de uma nova "sociedade de indivíduos" que "convocou a Internet e o crescente aparato de informação para nosso cotidiano" (ZUBOFF, 2019, p. 31-2).

> *When we look through this lens, we can see that those eager customers for Ford's incredible Model T and the new consumers of iPods and iPhones are expressions of the conditions of existence that characterized their era. In fact, each is the fruit of distinct phases of a centuries-long process known as "individualization" that is the human signature of the modern era. Ford's mass consumers were members of what has been called the "first modernity," but the new conditions of the "second modernity" produced a new kind of individual for whom the Apple inversion, and the many digital innovations that followed, would become essential. This second modernity summoned the likes of Google and Facebook into our lives, and, in an unexpected twist, helped*

[4] Tradução: Assim como a Ford explorou um novo consumo de massa, a Apple foi uma das primeiras a experimentar um sucesso comercial explosivo ao explorar uma nova sociedade de indivíduos e sua demanda por consumo individualizado (ZUBOFF, 2019, p. 29-30).

[5] Original: "*The opposing vector belongs to the decades-long elaboration and implementation of the neoliberal economic paradigm: its political economics, its transformation of society, and especially its aim to reverse, subdue, impede, and even destroy the individual urge toward psychological self-determination and moral agency*" (ZUBOFF, 2019, p. 30-1).

> *to enable the surveillance capitalism that would follow* (ZUBOFF, 2019, p. 32)[6].

Logo, a capacidade da Internet e dos novos mecanismos de transmissão de informação ofereceram às novas gerações mais oportunidades de conexão e compartilhamento de ideais, evidenciando o papel de protagonista do indivíduo na nossa era (ZUBOFF, 2019, p. 35-7).

Nesse sentido, o advento do computador pessoal na década de 1970 foi fundamental para a concretização dos novos padrões sociais da segunda modernidade. Mais especificamente, o *Apple II* (projetado por Steve Wozniak, o cofundador menos conhecido da Apple) "transformou a computação pessoal, até então um obscuro passatempo de aficionados, num fenômeno de alcance nacional" capaz de "revolucionar não só a computação como também as comunicações, a cultura, o entretenimento, os negócios – em suma, todos os aspectos produtivos da vida nos Estados Unidos" (WU, 2012).

Diferente de outras mídias como a televisão, o telefone e o rádio cujos inventores "possuíam o controle e o poder das novas tecnologias no interior de gigantescas instituições", onde "[i]novação gerava indústria, e indústria gerava consolidação", o computador pessoal dava ao indivíduo o controle absoluto da informação. Dessa forma, respondendo à IBM, cujos produtos eram tão caros que somente universidades, grandes empresas e governos podiam custear, a Apple democratizou a tecnologia proporcionando que mais pessoas pudessem participar desse novo momento histórico baseado no digital, descentralizando o poder da informação (WU, 2012).

A transparência inédita do modelo aberto do *Apple II* "[c]om fendas para acomodar qualquer tipo de dispositivo periférico e um sistema operacional que deixava o usuário programar a máquina como quisesse", foi posteriormente

---

[6] Tradução: Quando olhamos através dessa lente, podemos ver que aqueles clientes ansiosos pelo incrível Modelo T da Ford e os novos consumidores de *iPods* e *iPhones* são expressões das condições de existência que caracterizaram sua era. Na verdade, cada um é fruto de fases distintas de um processo secular conhecido como "individualização", que é a assinatura humana da era moderna. Os consumidores de massa da Ford eram membros do que foi chamado de "primeira modernidade", mas as novas condições da "segunda modernidade" produziram um novo tipo de indivíduo para quem a inversão da Apple e as muitas inovações digitais que se seguiram se tornariam essenciais. Esta segunda modernidade convocou empresas como o Google e o Facebook em nossas vidas e, em uma reviravolta inesperada, ajudou a possibilitar o capitalismo de vigilância que se seguiria (ZUBOFF, 2019, p. 32).

simulada pelo *Windows* que apresentava a vantagem de "funciona[r] em qualquer computador, admiti[r] qualquer tipo de *software* e tinha *interface* com qualquer impressora, modem ou outro *hardware*". E enquanto Steve Jobs decidiu com o lançamento do *Mac* que a empresa não mais continuaria com o modelo aberto, "[o] *Windows* ficou com o mercado em que a Apple fora pioneira baseando-se nas ideias com que ela começara" e, desde então, os modelos abertos representam uma parcela bem mais significativa da economia, reafirmando a máxima "'Aberto ganha de fechado', sugerindo que Wozniak tinha razão desde o começo" (WU, 2012).

No entanto, "[q]ualquer rede precisa ter uma forma de conectar seus usuários" e o Google se empenhou em oferecer esses serviços na Internet. Entrar em contato com alguém na era pré-computador dependia de um telefonista e uma rede complexa de cabos. Agora, basta procurar "o interlocutor pelo nome (digitando 'Ford Motor Company', por exemplo), e o Google mostra a maneira de se conectar com ele pela *web*" (WU, 2012).

Tal revolução, porém, só foi possível devido ao trabalho do físico Tim Berners-Lee que, durante o verão de 1980, "assumiu uma missão solo durante seu tempo livre: escrever um programa de computador para organizar a informação, a semente do que afinal iria florescer como a *World Wide Web*". Nomeado "*Enquire – Enquire Within Upon Everything*" como uma espécie de homenagem a um guia vitoriano sobre vida doméstica, o modelo "evoluiria naquilo que se tornou o maior repositório do mundo de respostas às caóticas perguntas sobre a vida", e dez anos depois Berners-Lee "escreveu um padrão (o *Hyper Text Markup Language*, ou *html*) e publicou as primeiras páginas da *web*", em 1990. Nesse mesmo momento, a *web* se popularizou e logo o *html* também (WU, 2012).

> Acessada por um navegador, a *web* originalmente não passava de um acordo para armazenar toda a informação num formato comum (*html*), combinado com maneiras de conectar pedaços de informação por intermédio dos chamados hiperlinks. O valor supremo da *web* era, e ainda é, sua universalidade. A ideia, como me contou Tim Berners-Lee, era que "a *web* deve funcionar com tudo: qualquer *hardware*, qualquer *software*, qualquer linguagem, todos os tipos diferentes de mídia, qualquer qualidade de dados, ser acessível a pessoas portadoras de deficiências e valer em qualquer cultura. Não apenas em diferentes linguagens, mas em diferentes culturas" (WU, 2012).

Tal princípio de universalidade é o que possibilitou a popularização dessa tecnologia no nosso cotidiano, revolucionando as relações econômicas e sociais da

segunda modernidade. Nesse sentido, criado na Universidade de Stanford, o Google, com sua missão de "'organizar a informação do mundo'" foi fundamental para a viabilização do acesso do público em geral à *web* (WU, 2012).

Pode-se dizer, inclusive, que o Google tinha como objetivo o mesmo que os *encyclopédistes* do século XVIII. Assim como Jean D'Alembert e Denis Diderot – alguns dos principais nomes envolvidos na criação da Enciclopédia –, a fundação do Google foi motivada pela criação de uma "estrutura universal de conhecimento" enquanto um empreendimento comercial. Para isso, novas tecnologias foram necessárias em ambos os casos, como novos meios de produção e de sistemas comerciais, e novas formas de compartilhamento desses mecanismos foram cunhadas (FINN, 2017, p. 68-71).

Contudo, há uma importante diferença: enquanto as técnicas empregadas pelos teóricos franceses eram conhecidas pelo público, os métodos do Google permanecem secretos, escondendo suas ambiguidades e controvérsias como uma prática importante para a manutenção do negócio baseado na vigilância. Ademais, os usuários do Google geralmente não usam a ferramenta para encontrar algo que estaria em uma enciclopédia, pois as perguntas feitas são de cunho muito mais pessoal do que um manual poderia responder. Segundo o antigo *CEO* da Google Eric Schmidt, "*I actually think most people don't want Google to answer their questions. They want Google to tell them what they should be doing next*"[7] (THE WALL STREET JOURNAL, 2010). O que se espera da Enciclopédia moderna, então, é a capacidade de antecipar o que o usuário ainda não sabe que deseja e, para realizar esse fim, é preciso saber o máximo possível sobre ele. "*For Google, the logic of the quest means that its effort to reach a state of universal knowledge also requires the achievement of perfect self-knowledge, of anticipating its users' needs and queries*"[8] (FINN, 2017, p. 72-3).

Segundo Ed Finn (2017), fundador e diretor do Center for Science and the Imagination da Arizona State University (Estados Unidos), há um certo aspecto

[7] Tradução: Na verdade, acho que a maioria das pessoas não quer que o Google responda às suas perguntas. Eles querem que o Google diga o que eles devem fazer a seguir (THE WALL STREET JOURNAL, 2010).

[8] Tradução: Para o Google, a lógica da busca significa que seu esforço para alcançar um estado de conhecimento universal também requer a obtenção de um autoconhecimento perfeito, de antecipar as necessidades e dúvidas de seus usuários (FINN, 2017, p. 72-3).

religioso na computação. Assim como a escrita e a leitura eram habilidades restritas aos integrantes da Igreja durante a Idade Média, hoje, a capacidade de entender e falar a linguagem do computador é dominada por poucos, e essa concentração de informação cria uma acentuada assimetria de poder. Uma vez que a computação permite a concentração de todos os ramos do conhecimento sob uma única "árvore", ela pode ser vista como o "solvente universal capaz de compreender qualquer sistema complexo, da consciência humana ao universo em si" (FINN, 2017, p. 8-9, tradução minha[9]).

Com isso, a computação tem consequências sobre todos os aspectos da vida humana, incluindo questões materiais como a economia, mas também imateriais como a cultura, podendo ditar como nos relacionamos com a tecnologia, e consequentemente, modificando nossa agência. Para o autor, "*[t]he theocracy of computation will not merely change the world but evolve it, and it will open new possibilities for users, linking proprietary commerce and individual freedom. (...) The algorithm offers us salvation, but only after we accept its terms of service*"[10] (FINN, 2017, p. 9).

Ademais, dada a assimetria de poder, também semelhante ao período da Idade Média, uma espécie de magia tende a ser associada à tecnologia. "*We believe in the power of code as a set of magical symbols linking the invisible and visible, echoing our long cultural tradition of logos, or language as an underlying system of order and reason, and its power as a kind of sorcery*."[11] Já que muitas pessoas não falam a "língua do computador" ou pouco sabem sobre os processos envolvidos na computação e cada vez mais nossas vidas são mediadas por tais mecanismos, tende-se a não questionar os processos por trás da tecnologia, o que contribui para

[9] Original: "*Computation offers a pathway for consilience, or the unification of all fields of knowledge into a single tree: an ontology of information founded on the idea that computation is a universal solvent that can untangle any complex system, from human consciousness to the universe itself*" (FINN, 2017, p. 8).

[10] Tradução: a teocracia da computação não apenas mudará o mundo, mas o evoluirá, e abrirá novas possibilidades para os usuários, vinculando comércio proprietário e liberdade individual. (…) O algoritmo nos oferece a salvação, mas só depois de aceitarmos seus termos de serviço (FINN, 2017, p. 9).

[11] Tradução: Acreditamos no poder do código como um conjunto de símbolos mágicos que ligam o invisível e o visível, ecoando nossa longa tradição cultural de logos, ou linguagem como um sistema subjacente de ordem e razão, e seu poder como um tipo de feitiçaria (FINN, 2017, p. 34).

a alienação da população quanto à vigilância presente nesses processos (FINN, 2017, p. 34).

E para atender aos desejos do público de ter suas perguntas respondidas antes de serem formuladas – como Schmidt coloca –, o Google deixa de ser uma empresa focada em acesso à informação e passa a agir como um ser pensante capaz de modificar nosso comportamento e forma de pensar devido à sua capacidade de agência e suas estruturas de influência (FINN, 2017, p. 66-7).

Isto é, para realmente conhecer o usuário, o Google depende de uma estrutura complexa de vigilância permanente composta por aplicativos de busca, entretenimento, transporte, comunicação, saúde e educação, pois quanto maior o volume e a qualidade de dados acumulados, mais detalhado é o perfil desenhado sobre o indivíduo e maior a capacidade preditiva da empresa.

> *Google's near omnipresence online, its imbrication in countless cultural systems that do not merely enable but effectively define certain cultural fields of play for billions of people, make this more than just a suggestion service or even a sophisticated form of advertising. The Google culture machine is assembling a map that at times threatens to upstage the territory* (FINN, 2017, p. 74)[12].

Shoshana Zuboff nomeia esse novo modelo econômico de "capitalismo de vigilância": caracterizado por uma nova linguagem – o texto eletrônico – que media os principais aspectos da vida em sociedade graças à proliferação de celulares, câmeras, computadores e sensores capazes de capturar todo tipo de dados pessoais. Como consequência, "*both the world and our lives are pervasively rendered as information*"[13] (ZUBOFF, 2019, p. 182-3) e assim, os aspectos mais básicos da sociedade como leis, instituições, linguagem, tradições e bens culturais são digitalizados e em seguida, devolvidos à sociedade por meio do filtro de "algoritmos inteligentes" empregados para controlar uma gama de funções comerciais, governamentais e sociais que se multiplica rapidamente (GILLINGS et al, 2016, p. 185).

---

[12] Tradução: A quase onipresença *online* do Google, sua imbricação em incontáveis sistemas culturais que não apenas permitem, mas efetivamente definem certos campos culturais de jogo para bilhões de pessoas, tornam isso mais do que apenas um serviço de sugestão ou mesmo uma forma sofisticada de publicidade. A máquina cultural do Google está montando um mapa que às vezes ameaça ofuscar o território (FINN, 2017, p. 74).

[13] Tradução: tanto o mundo quanto nossas vidas são sistematicamente processados como informações (ZUBOFF, 2019, p. 182-3).

Uma das principais características dos mecanismos do capitalismo de vigilância, então, diz respeito ao "problema dos dois textos." Segundo Zuboff, o primeiro texto é aquilo que nós produzimos e enxergamos: são páginas de *blogs*, *posts* em redes sociais, *streaming* de músicas e vídeos, troca de *e-mails* que servem como matéria-prima para o segundo texto, o "texto sombra" ("*shadow text*"). Invisível aos usuários, este diz respeito às informações adquiridas pelas empresas conforme interagimos com a Internet em nossas rotinas: são nossos padrões de busca, como *sites* mais visitados; a maneira pela qual nos deslocamos, se de carro, a pé ou transporte público; os lugares que frequentamos como restaurantes, lojas, academia; e hábitos de compras como uso de crédito ou débito, onde e quando compramos (ZUBOFF, 2019, p. 185-6).

Dessa forma, conforme os atores do capitalismo de vigilância controlam a produção de ambos os textos há uma assimetria de conhecimento e poder capaz de produzir uma "divisão do aprendizado" a qual desconhecemos e, portanto, não temos os meios para enfrentar. Isto é, à medida que nossas interações com a Internet são mediadas por algumas poucas empresas – as chamadas *big tech* –, estas detêm o segundo texto, as informações necessárias para prever nosso comportamento e, portanto, modificá-lo (ZUBOFF, 2019, p. 183).

Nesse processo, muito conhecimento técnico é exigido para desenvolver os algoritmos mais precisos e sofisticados e, então, nos últimos anos, os especialistas em inteligência artificial foram cooptados pelas *big tech*. Ao invés de desenvolver soluções para problemas coletivos como distribuição de alimento e geração de energia limpa, os mais versados na linguagem do computador são sistematicamente recrutados por empresas como o Google, que nos últimos anos se tornou o maior contribuidor para as revistas científicas de maior prestígio e triplicou o número de cientistas em "*machine intelligence*", alimentando o ciclo de coleta e análise de dados em nome da previsão e controle do comportamento humano (ZUBOFF, 2019, p. 189-90).

2.2 Google: pioneiro do capitalismo de vigilância

Como mencionado anteriormente, o princípio original do Google era "organizar a informação mundial", proporcionando aos usuários acesso à *web* (WU, 2012). Num primeiro momento, então, em prol de um melhor serviço ao usuário, as informações do "texto sombra" eram usadas com o objetivo de oferecer respostas mais acuradas às pesquisas. Com isso, havia um balanço de poder entre o Google e o usuário à medida que ambos se beneficiavam dessa relação mútua. "*People were treated as ends in themselves, the subjects of a nonmarket, self-contained cycle that was perfectly aligned with Google's stated mission*"[14] (ZUBOFF, 2019, p. 69-70).

Porém, devido à pressão dos investidores, especialmente após a "Crise das ponto com" para encontrar novas maneiras de lucrar, foi adotada uma estratégia de abrir o *site* para propagandas direcionadas. Pois, concluiu-se que uma vez que haveriam anúncios, esses deveriam ser relevantes. "*Ads would no longer be linked to keywords in a search query, but rather a particular ad would be 'targeted' to a particular individual. Securing this holy grail of advertising would ensure relevance to users and value to advertisers*"[15] (ZUBOFF, 2019, p. 74).

Assim, além de usar o "texto sombra" como uma forma de promover segurança ao trabalhar junto ao governo estadunidense, o Google inaugurou esse novo modelo econômico baseado na coleta de informações comportamentais dos usuários e venda de acuracidade e previsibilidade para os anunciantes, o que iria conferir à empresa uma vantagem competitiva como nunca antes vista (em 2004, a *run rate* era de US$1 milhão por dia, e em 2010, os lucros ultrapassavam os US$10 bilhões), mas também determinaria os rumos da economia no século XXI (ZUBOFF, 2019, p. 81-3).

> *As a Bloomberg journalist explained in 2006, "Google maximizes the revenue it gets from that precious real estate by giving its best position to the advertiser who is likely to pay Google the most in total, based on the price per click multiplied by Google's estimate of the likelihood that someone will actually click on the ad." That pivotal multiplier was the result of Google's advanced computational capabilities trained on its most significant and secret discovery: behavioral surplus. From this point forward, the combination of ever-increasing machine intelligence*

[14] Tradução: As pessoas eram tratadas como fins em si mesmas, sujeitos de um clico não-mercadológico e independente que estava perfeitamente alinhado com a missão declarada do Google (ZUBOFF, 2019, p. 69-70).

[15] Tradução: Os anúncios não seriam mais vinculados a palavras-chave em uma consulta de pesquisa, mas um determinado anúncio seria "direcionado" para um determinado indivíduo. Proteger esse Santo Graal da publicidade garantiria relevância para os usuários e valor para o anunciante (ZUBOFF, 2019, p. 74).

> *and ever-more-vast supplies of behavioral surplus would become the foundation of an unprecedented logic of accumulation. Google's reinvestment priorities would shift from merely improving its user offerings to inventing and institutionalizing the most far-reaching and technologically advanced raw material supply operations that the world had ever seen. Henceforth, revenues and growth would depend upon more behavioral surplus* (ZUBOFF, 2019, p. 76-7)[16].

De forma simplificada, "cada vez que um usuário consulta o mecanismo de pesquisa do Google, o sistema apresenta simultaneamente uma configuração específica de um determinado anúncio." Assim, para aumentar ao máximo a acuracidade dessas previsões, são analisados dados muito além dos termos de busca: as chamadas "informações de perfil do usuário" ("*user profile information*") conferem uma certeza matemática que elimina suposições e resulta em "muito menos desperdício no orçamento de publicidade" (ZUBOFF, 2019, p. 78, tradução minha[17]).

Além disso, como mencionado anteriormente, devido à recém-formada parceria com as agências de segurança, e às consequentes proteções legais impostas sobre as empresas de tecnologia, o Google prosperou nesse cenário, ignorando possíveis dilemas éticos e eventuais questionamentos sobre direitos de decisão dos indivíduos. "*This Google is the superpower that establishes its own values and pursues its own purposes above and beyond the social contracts to which others are bound*"[18] (ZUBOFF, 2019, p. 81).

Nesse sentido, ao invés de servir ao usuário, o Google decide que estes se tornarão os meios para satisfazer a demanda por anunciantes ansiosos em adquirir

---

[16] Tradução: Como explicou um jornalista da Bloomberg em 2006, "o Google maximiza a receita que obtém desse precioso empreendimento, dando sua melhor posição ao anunciante que provavelmente pagará ao Google mais no total, com base no preço por clique multiplicado pela estimativa do Google da probabilidade de que alguém realmente clique no anúncio." Esse multiplicador fundamental foi o resultado dos recursos computacionais avançados do Google treinados em sua descoberta mais significativa e secreta: o excedente comportamental. Desse ponto em diante, a combinação de inteligência da máquina cada vez maior e suprimentos cada vez mais vastos de excedentes comportamentais se tornaria a base de uma lógica de acumulação sem precedentes. As prioridades de reinvestimento do Google passariam de meramente melhorar suas ofertas aos usuários para inventar e institucionalizar as operações de fornecimento de matéria-prima de maior alcance e tecnologicamente avançadas que o mundo já viu. Doravante, receitas e crescimento dependeriam de mais excedente comportamental (ZUBOFF, 2019, p. 76-7).

[17] Original: "*New data sets were compiled that would dramatically enhance the accuracy of these predictions. These data sets were referred to as "user profile information" or "UPI." These new data meant that there would be no more guesswork and far less waste in the advertising budget. Mathematical certainty would replace all of that*" (ZUBOFF, 2019, p. 78).

[18] Tradução: Este Google é a superpotência que estabelece seus próprios valores e busca seus próprios objetivos acima e além dos contratos sociais aos quais os outros estão vinculados (ZUBOFF, 2019, p. 81).

novos mercados e adota uma estratégia de total segredo não só para que outros não adotem a mesma estratégia – o que acaba acontecendo pouco tempo depois –, mas principalmente para preservar a "assemblagem de vigilância." Para garantir que os usuários continuassem usando os serviços Google, estes não poderiam saber que sua privacidade era constantemente violada ao terem seus dados coletados sem o seu consentimento e usados em benefício de terceiros (ZUBOFF, 2019, p. 89-90).

2.3 Facebook: o "*Big Brother*" da segunda modernidade

No mesmo ano em que o Google abre seu capital, o Facebook foi criado. E o que começou como uma brincadeira de um universitário, anos mais tarde se tornou um dos maiores responsáveis pela disseminação do capitalismo de vigilância. Para "conectar todas as pessoas do mundo", pouco depois de abrir o *site* para o público em geral (não mais somente quem tivesse um *e-mail* de universidade), Mark Zuckerberg lançou uma grande plataforma de anúncios. Com pouca aprovação dos usuários, o *Beacon* "compartilhava automaticamente as transações de sites parceiros com todos os 'amigos' do usuário", mesmo que ele não estivesse conectado ao Facebook e sem a opção de escolher participar ("*opt-in function*"), o que levou a reclamações por parte dos usuários, mas serviu de protótipo para um novo modelo de negócios (ZUBOFF, 2019, p. 91-2, tradução minha[19]).

Pois, ao perceber o potencial de serviço de propaganda em uma rede social – onde sabe-se informações como idade, localização, mas também preferências e lista de "amigos" –, uma cultura de compartilhamento entre os usuários foi rapidamente incentivada, bem como a inserção de anunciantes no Facebook, aproximando-os dos usuários. Assim, o Facebook adere às estratégias do Google de usar os usuários como matéria-prima para seus reais produtos, as capacidades preditivas sobre nosso comportamento, vendidos para os anunciantes, seus reais clientes (ZUBOFF, 2019, p. 92-4).

[19] Original: "'*Our mission is to connect every person in the world. You don't do that by having a service people pay for,' he insisted. (...) Six months later, in November, he launched his big advertising product, Beacon, which would automatically share transactions from partner websites with all of a user's 'friends.' These posts would appear even if the user was not currently logged into Facebook, without the user's knowledge or an opt-in function* (ZUBOFF, 2019, p. 91-2).

Portanto, a coleta de dados é uma das etapas cruciais para o sucesso da empresa. Além da "quantidade astronômica de informação sobre as pessoas, suas redes sociais, suas preferências e antipatias declaradas" conhecidas devido à quase onipresença do botão do Facebook, a empresa passa a capturar dados sobre o comportamento *offline* das pessoas, se aliando a "grandes empresas como a Experian, que há décadas monitora as compras dos consumidores por meio de relações com firmas de marketing direto, empresas de cartão de crédito e varejistas." Com esse tipo de informação, então, "o Facebook poderia combinar a identidade de cada usuário ao identificador único do respectivo aparelho de celular", traçando um perfil detalhado de cada um, pois, além dos hábitos *online* (como *posts* curtidos e *sites* visitados), passa-se a conhecer a renda, o estado civil, nível de escolaridade e todo o histórico de compras do usuário (LANCHESTER, 2017).

> O que isso quer dizer é que, mais do que vender anúncios, a principal atividade do Facebook é a vigilância. Na verdade, ele é a maior empresa com base na vigilância de toda a história da humanidade. Ele sabe de muito mais a nosso respeito que o governo mais invasivo jamais soube acerca de seus cidadãos. (...) Não sei se já existiu tamanha desconexão entre o que uma empresa alega fazer – "conectar", "construir comunidades" – e a realidade de sua prática comercial (LANCHESTER, 2017).

E com a implementação do "*News feed*", uma nova forma de manipulação é inaugurada, pois há um maior incentivo para que os usuários entrem no *site* com mais frequência. Orientado pelos interesses comerciais do Facebook, aquilo que aparece para cada usuário é determinado por seus gostos e amigos, mas principalmente pelo "texto sombra" de cada um (LANCHESTER, 2017; ZUBOFF, 2019). Porém, vale ressaltar ainda que tanto notícias sobre amigos quanto anúncios aparecem da mesma forma no *feed*, tornando a propaganda cada vez mais sutil e contribuindo para o incentivo à fofoca, ao monitoramento das ações de seus "amigos" (COHEN, 2008, p. 12).

Funções como o *feed* de notícias do Facebook (reproduzidas por redes sociais como Instagram, Twitter e outras), então, são uma forma de atrair a atenção do usuário com o objetivo de que este continue na plataforma pelo maior tempo possível, alimentando cada vez mais o "texto sombra". Segundo Tim Wu (2016), a indústria da atenção vem cada vez mais cooptando nossas rotinas em troca de divertimento e conveniência, numa barganha extremamente desproporcional. "*In*

the process, as a society and individually, we have accepted a life experience that is in all of its dimensions—economic, political, social, any way you can think of—mediated as never before in human history"[20] (WU, 2016).

Uma das principais características dessa indústria, o elemento da propaganda, então, passou a ser fortemente adotado pelo setor industrial após as Guerras Mundiais – um dos fenômenos mais influentes sobre a "segunda modernidade" – e a atenção passou a ser vista cada vez mais como uma *commodity*. "*Beginning with radio, each new medium would attain its commercial viability through the resale of what attention it could capture in exchange for its 'free' content*"[21] (WU, 2016; ZUBOFF, 2019).

Esse comércio foi tão bem pensado, que sua presença é minimamente notada – ou questionada – ao longo das gerações. Ao adentrar segmentos anteriormente não explorados economicamente e sutilmente fazer parte do cotidiano das pessoas, nossa atenção vem sendo cooptada e nossos dados roubados em troca de anúncios que modificam nosso comportamento.

> *As we shall see, the winning strategy from the beginning has been to seek out time and spaces previously walled off from commercial exploitation, gathering up chunks and then slivers of our un-harvested awareness. Within living memory it was thought that families would never tolerate the intrusion of broadcasting in the home. An earlier generation would find it astonishing that, without payment or even much outcry, our networks of family, friends, and associates have been recruited via social media to help sell us things. Now, however, most of us carry devices on our bodies that constantly find ways to commercialize the smallest particles of our time and attention. Thus, bit by bit, what was once shocking became normal, until the shape of our lives yielded further and further to the logic of commerce—but gradually enough that we should now find nothing strange about it* (WU, 2016)[22].

[20] Tradução: No processo, como sociedade e individualmente, aceitamos uma experiência de vida que está em todas as suas dimensões - econômica, política, social, de qualquer maneira que você possa imaginar - mediada como nunca antes na história humana (WU, 2016).
[21] Tradução: Começando com o rádio, cada novo meio alcançaria sua viabilidade comercial por meio da revenda de toda atenção que poderia captar em troca de seu conteúdo "gratuito" (WU, 2016).
[22] Tradução: Como veremos, a estratégia vencedora desde o início tem sido buscar tempo e espaços antes isolados da exploração comercial, reunindo pedaços e, em seguida, lascas de nossa consciência não colhida. Dentro da memória viva, pensava-se que as famílias nunca tolerariam a intrusão da transmissão em casa. Uma geração anterior acharia surpreendente que, sem pagamento ou mesmo muito clamor, nossas redes de familiares, amigos e associados tenham sido recrutadas por meio da mídia social para ajudar a nos vender coisas. Agora, porém, a maioria de nós carrega dispositivos em nossos corpos que constantemente encontram maneiras de comercializar as menores partículas de nosso tempo e atenção. Assim, pouco a pouco, o que antes era chocante tornou-se normal, até que a forma de nossas vidas cedeu cada vez mais à lógica do comércio - mas gradualmente o suficiente para que agora não encontrássemos nada de estranho nisso (WU, 2016).

Porém, à medida que cada vez mais objetos conectados à Internet fazem parte do nosso cotidiano, mais nos tornamos reféns desse sistema, pois "inteligência" é sinônimo de "rendição": quanto mais sobre nós é conhecido por esses objetos, mais nosso comportamento é manipulado pelo capitalismo de vigilância, como se vivêssemos em um grande cassino disfarçado (ZUBOFF, 2019, p. 238).

Mas não são somente os aparelhos da "*Internet of Things*" como geladeiras *smart* ou carros autônomos que atuam nos cassinos do século XXI: os *smartphones* são as maiores fontes de informação sobre uma pessoa, pois indicam nossa localização o tempo todo e se tornaram quase uma extensão dos corpos, estando presentes em virtualmente qualquer momento do dia de alguém, desde o acordar até o deitar. Consequentemente, nossos corpos são reimaginados como um objeto comportamental a ser monitorado e manipulado (ZUBOFF, 2019, p. 242).

É importante lembrar, no entanto, que muitos desses objetos são essenciais para algumas pessoas e que temos o direito de usufruir de seus benefícios, desde que sejamos informados sobre seus custos. A tecnologia não é um vilão que devemos combater, mas uma aliada nas lutas do nosso tempo que foi capturada pelo interesse comercial de algumas empresas.

Todavia, devido à enorme assimetria de poder entre essas empresas e a população em geral, retomar o controle da tecnologia não será fácil. Como Wu (2016) coloca, historicamente, as lutas contra a indústria da atenção evidenciam o quanto somos fracos.

> *Individually, we have the power to ignore, tune out, and unplug. At certain times over the last century, the industry has asked too much and offered too little in return, or even been seen to violate the public's trust outright. At such moments, the bargain of the attention merchants is beset with a certain "disenchantment," which, if popular grievance is great enough, can sometimes turn into a full-fledged "revolt." During those revolts—of which there have been several over the last century—the attention merchants and their partners in the advertising industry have been obliged to present a new deal, revise the terms of the arrangement. We may, in fact, be living in such a time today, at least in those segments of the population committed to cord-cutting, ad-avoiding, or unplugging. We are certainly at an appropriate time to*

> *think seriously about what it might mean to reclaim our collective consciousness* (WU, 2016)[23].

Lutar contra empresas como o Google, cujos "fundadores construíram um guia corporativo que lhes deu controle absoluto na esfera do mercado e também a liberdade na esfera pública", apresenta uma série de desafios. Ao se aproveitarem da falta de limites legais impostos sobre o ciberespaço, essas empresas se apropriaram deste e o exploraram como desejavam, assim como os colonizadores europeus do século XIX na África e Ásia (ZUBOFF, 2019, p. 103, tradução minha[24]).

Ademais, devido à rapidez da tecnologia, várias tentativas de regular suas atividades falharam. Pois, o processo de desenvolvimento, votação, aprovação e implementação de leis é infinitamente mais lento do que a capacidade de adaptação do capitalismo de vigilância e este luta constantemente para que nenhum impeditivo afete seu funcionamento. "*Google and Facebook vigorously lobby to kill online privacy protection, limit regulations, weaken or block privacy-enhancing legislation, and thwart every attempt to circumscribe their practices because such laws are existential threats to the frictionless flow of behavioral surplus*"[25] (ZUBOFF, 2019, p. 105).

> *This market form must either gird itself for perpetual conflict with the democratic process or find new ways to infiltrate, seduce, and bend democracy to its ends if it is to fulfill its own inner logic. The survival and success of surveillance capitalism depend upon engineering collective agreement through all available means while simultaneously*

[23] Tradução: Individualmente, temos o poder de ignorar, desligar e desconectar. Em certos momentos do século passado, a indústria pediu muito e ofereceu muito pouco em troca, ou mesmo foi vista como uma violação da confiança do público de uma vez. Nesses momentos, a barganha dos mercadores de atenção é cercada por um certo "desencanto", que, se a reclamação popular for grande o suficiente, às vezes pode se transformar em uma "revolta" completa. Durante essas revoltas - das quais ocorreram várias ao longo do século passado - a atenção dos comerciantes e seus parceiros na indústria da publicidade foram obrigados a apresentar um novo acordo, revisar os termos do acordo. Podemos, de fato, estar vivendo em tal época hoje, pelo menos naqueles segmentos da população comprometidos com o corte do cabo, a evasão de publicidade ou o desligamento. Certamente estamos em um momento apropriado para pensar seriamente sobre o que pode significar reivindicar nossa consciência coletiva (WU, 2016).

[24] Original: "*Google's founders constructed a corporate form that gave them absolute control in the market sphere, and they also pursued freedom in the public sphere*" (ZUBOFF, 2019, p. 103).

[25] Tradução: O Google e o Facebook vigorosamente fazem lobby para eliminar a proteção da privacidade online, limitar as regulamentações, enfraquecer ou bloquear a legislação que aumenta a privacidade e frustrar todas as tentativas de circunscrever suas práticas porque essas leis são ameaças existenciais ao fluxo sem atrito do excedente comportamental (ZUBOFF, 2019, p. 105).

> *ignoring, evading, contesting, reshaping, or otherwise vanquishing laws that threaten free behavioral surplus* (ZUBOFF, 2019, p. 105)[26].

Nesse sentido, as empresas do capitalismo de vigilância advogam cada vez mais pelo direito de se autorregularem, o que, desde 2004 com a abertura do Google e sua parceria com as agências de segurança, foi extremamente encorajado pelo governo estadunidense como a "ferramenta mais eficiente para regulação sem coerção e o antídoto para qualquer inclinação ao coletivismo e centralização de poder" (ZUBOFF, 2019, p. 107-8, tradução minha[27]). No entanto, essa postura coloca a privacidade como um bem a ser negociado e evidencia a desproporcionalidade de poder entre os fundadores dessas empresas e a população.

> *Surveillance capitalism's ability to keep democracy at bay produced these stark facts. Two men at Google who do not enjoy the legitimacy of the vote, democratic oversight, or the demands of shareholder governance exercise control over the organization and presentation of the world's information. One man at Facebook who does not enjoy the legitimacy of the vote, democratic oversight, or the demands of shareholder governance exercises control over an increasingly universal means of social connection along with the information concealed in its networks* (ZUBOFF, 2019, p. 127)[28].

Em última instância, corremos o risco de viver vidas que nunca escolhemos ter (WU, 2016). Como vivemos em uma "assemblagem de vigilância" e desconhecemos os reais mecanismos envolvidos em nossas interações com a Internet ou os riscos implícitos desse processo, fazer frente ao capitalismo de vigilância é um desafio.

---

[26] Tradução: Essa forma de mercado deve se preparar para o conflito perpétuo com o processo democrático ou encontrar novas maneiras de se infiltrar, seduzir e dobrar a democracia até o fim, se quiser cumprir sua própria lógica interna. A sobrevivência e o sucesso do capitalismo de vigilância dependem da engenharia de acordos coletivos por meio de todos os meios disponíveis, ao mesmo tempo em que ignora, evita, contesta, reformula ou, de outra forma, derrota as leis que ameaçam o excedente comportamental livre (ZUBOFF, 2019, p. 105).

[27] Original: "*By the time of Google's public offering in 2004, self-regulation was fully enshrined within government and across the business community as the single most effective tool for regulation without coercion and the antidote to any inclination toward collectivism and the centralization of power*" (ZUBOFF, 2019, p. 107-8).

[28] Tradução: A habilidade do capitalismo de vigilância de manter a democracia sob controle produziu esses fatos marcantes. Dois homens do Google que não gozam da legitimidade do voto, da supervisão democrática ou das demandas de governança de acionistas exercem controle sobre a organização e a apresentação das informações do mundo. Um homem no Facebook que não goza da legitimidade do voto, da supervisão democrática ou das demandas de governança de acionistas exerce controle sobre um meio cada vez mais universal de conexão social junto com as informações ocultas em suas redes (ZUBOFF, 2019, p. 127).

CAPÍTULO 3

O Tecnocontrole e a Degradação da Democracia

Entender as questões sociais existentes hoje sem levar em conta o papel da tecnologia é ignorar um aspecto determinante da vida em sociedade no século XXI. Como apontado pelo sociólogo Manuel Castells (1999), "o dilema do determinismo tecnológico é, provavelmente, um problema infundado, dado que a tecnologia *é* a sociedade, e a sociedade não pode ser entendida ou representada sem suas ferramentas tecnológicas." Isto é, o fato de que a Internet surgiu como um projeto militar do governo estadunidense a partir da segunda metade do século XX, mas só se popularizou graças a algumas empresas baseadas na Califórnia evidencia como aspectos culturais como "liberdade, inovação individual e iniciativa empreendedora oriunda dos *campi* norte-americanos da década de 1960" são determinantes nesse processo histórico (CASTELLS, 1999, p. 43, grifos originais).

Segundo o autor, "a habilidade ou inabilidade de as sociedades dominarem a tecnologia e, em especial, aquelas (...) que são estrategicamente decisivas em cada período histórico, traça seu destino a ponto de podermos dizer que (...) a tecnologia (ou sua falta) incorpora a capacidade de transformação das sociedades" (CASTELLS, 1999, p. 44-5). Portanto, a completa dominação da tecnologia por algumas poucas empresas – as *big tech* – evidencia o poder que estas têm sobre a sociedade – em especial, quanto à formação de identidades – e, consequentemente, sobre a política.

Para Castells, "as sociedades informacionais parecem (ser caracterizadas) pela preeminência da identidade como seu princípio organizacional" (1999, p. 57). À medida que os indivíduos convivem mais com tecnologias de informação e comunicação (TICs), esses elementos se tornam parte do cotidiano e influenciam a maneira como significados são construídos e reconhecidos. Nesse sentido, as crianças nascidas a partir de meados da década de 1990 (Geração Z) e que cresceram com computadores, *smartphones*, "brinquedos inteligentes" como bichos de pelúcia controlados por aplicativo e, principalmente, as redes sociais são extremamente afetadas conforme suas relações sociais são mediadas por esses

mecanismos, alterando a maneira como enxergam o mundo e a si mesmas. Segundo o documentário *O dilema das redes* (2020), as taxas de depressão e ansiedade em adolescentes americanos aumentaram significativamente entre 2011-2013, assim como as taxas de automutilação não-fatal (cerca de 62% e 189% entre meninas de 15-19 anos e 10-14 anos, respectivamente) e suicídio (cerca de 70% e 151% entre meninas de 15-19 anos e 10-14 anos, respectivamente). Fenômeno que se deve, em grande parte, à maior presença de crianças e adolescentes nas redes sociais, onde a realidade é moldada de forma a simular a perfeição e todos parecem felizes o tempo todo.

Ademais, de acordo com Anthony Giddens (1990), a vigilância estatística ajuda a informar as pessoas sobre o mundo onde vivem; ou seja, informações sobre taxas de divórcio, por exemplo, podem influenciar a decisão de se casar ou não (GIDDENS, 1990). De forma semelhante, a observação da vida de outras pessoas por meio das redes sociais intensifica a vigilância na sociedade não só de maneira *top-down* – pelo Estado –, mas também a nível *bottom-up* e lateral, com consumidores monitorados a todo momento e indivíduos se assistindo realizar diversas atividades (WELLER, 2012, p. 62).

Isto é, "recentemente o controle e a vigilância da Internet deixaram de ser práticas exclusivas de Estados autoritários, tornando-se cada vez mais frequentes em países institucionalmente democráticos." Como as informações divulgadas por Edward Snowden em junho de 2013 evidenciam, o programa *PRISM* permitiu que a Agência de Segurança Nacional (NSA em inglês) tivesse "acesso direto a servidores de grandes empresas da Internet, sendo assim capaz de monitorar comportamentos de seus usuários em escala global", inclusive de membros de governos estrangeiros (BRUNO, 2013, p. 10).

Além disso, segundo Fernanda Bruno (2013), professora da Universidade Federal do Rio de Janeiro/UFRJ e Coordenadora do MediaLab e do CiberIDEA, "[a] expansão da videovigilância, notável nos grandes centros urbanos após os atentados de 11 de setembro de 2001 nos Estados Unidos, reorganiza as relações entre segurança e vigilância", deixando de focar somente em "populações e espaços classificados como perigosos ou suspeitos" e monitorando "toda sorte de espaço público, semipúblico e privado." Como consequência, a noção de vigilância passa

a ser "definida como a observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista produzir conhecimento e intervir sobre os mesmos, de modo a conduzir suas condutas" (BRUNO, 2013, p. 8; 18).

> *I do not want to argue here that all such monitoring is surveillance (...), but I would like to argue that, regardless of the direct aim of such monitoring of public goods, such as global environmental management, the forms of monitoring employed are biopolitical and surveillant. This is because: first, they are conducted with the ultimate aim of changing the behavior of human subjects either individually or in populations; second, they often have multiple purposes, only some of which relate to their ostensible public benefits; and third, they also have other indirect and unintentional effects on humans* (WOOD, 2012, p. 337)[1].

Com estimativas de que o número de objetos conectados à Internet deve ultrapassar o número de pessoas no planeta, chegando à marca dos 25 bilhões em 2020, consequentemente, o monitoramento do cotidiano chega a níveis sem precedentes (MAGRANI, 2017, p. 2). Assim, a privacidade vem se tornando um "problema político" (AGAR, 2003, p. 343) à medida que, nos últimos anos, crescem as preocupações quanto à segurança de centros de dados (WELLER, 2012, p. 62-3), mas principalmente devido à generalização da vigilância, motivada pela inexistência (ou quase) de medidas regulatórias quanto à atividade das *big tech.*

Vale destacar ainda que ao mesmo tempo que o capitalismo de vigilância monitora os indivíduos, estes são moldados por esse processo.

> *All surveillance implies not only observation of individuals and populations, but also the production of knowledge that allows their behavior to be governed. In the cyberspace environment, this knowledge is produced primarily by analysis of the huge mass of personal data in circulation. (...) But what kind of knowledge is produced? The epistemic model is also a taxonomic model. Mining of this data flow produces classifications that constitute a taxonomy of cyberspace users and extracts patterns related to their habits, preferences and behaviors* (BRUNO, 2012, p. 348)[2].

---

[1] Tradução: Não quero argumentar aqui que todo esse monitoramento é vigilância (...), mas gostaria de argumentar que, independentemente do objetivo direto desse monitoramento de bens públicos, como a gestão ambiental global, as formas de monitoramento empregadas são biopolíticas e vigilantes. Isso porque: primeiro, eles são conduzidos com o objetivo final de mudar o comportamento dos sujeitos humanos individualmente ou em populações; em segundo lugar, muitas vezes têm múltiplos propósitos, apenas alguns dos quais relacionados a seus ostensivos benefícios públicos; e terceiro, eles também têm outros efeitos indiretos e não intencionais em humanos (WOOD, 2012, p. 337).

[2] Tradução: Toda vigilância implica não só na observação de indivíduos e populações, mas também na produção de conhecimentos que permitam governar seus comportamentos. No ambiente do ciberespaço, esse conhecimento é produzido principalmente pela análise da enorme massa de dados

Nesse sentido, "as identidades projetadas nos perfis [dos usuários] constituem uma série de biografias proativas", modificadas à medida que as previsões comportamentais são cada vez mais precisas. De fato, o real poder do capitalismo de vigilância quanto à sua capacidade preditiva está não nessa habilidade em si, mas na "habilidade performativa de tornar realidade o que antes era mero potencial" (BRUNO, 2012, p. 349, tradução minha[3]).

"É nesse poder performativo e proativo que reside o perigo da mineração de dados e da criação de perfis" (BRUNO, 2012, p. 349, tradução minha[4]). Por um lado, as técnicas de *profiling* podem reforçar desigualdades sociais e perpetuar formas de discriminação; e por outro, há um incentivo ao consumo e à naturalização da vigilância (BRUNO, 2012).

Ademais, *"[w]hat appears at first blush to be a zero-sum game is in fact a set of interdependent relationships*"[5] (KERR & BARRIGAR, 2012, p. 386). Pois, com a globalização, as relações se tornam mais dispersas. Isto é, a relação entre informação e formação de identidades deixa de ser orientada exclusivamente pelo contexto local e familiar e passa a sofrer influência também de outras comunidades mais distantes geograficamente – e culturalmente. Porém, também é preciso levar em consideração o papel político dessa formação de identidades da segunda modernidade (ZUBOFF, 2019, p. 31-2), uma vez que "[c]onstruir uma identidade por meio do uso de representações simbólicas é uma questão de controle da informação". E, como o controle da informação vem sendo cooptado pelo capitalismo de vigilância, este tem o poder de distorcer, roubar e deletar nossa identidade (KERR & BARRIGAR, 2012, p. 386, tradução minha[6]), uma habilidade viabilizada pela própria arquitetura da computação:

---

pessoais em circulação. (...) Mas que tipo de conhecimento é produzido? O modelo epistêmico também é um modelo taxonômico. A mineração desse fluxo de dados produz classificações que constituem uma taxonomia dos usuários do ciberespaço e extrai padrões relacionados a seus hábitos, preferências e comportamentos (BRUNO, 2012, p. 348).

[3] Original: "*The power of the performative and oracular enunciation lies not in the ability to predict a necessary future but in the performative ability to turn into reality what was merely a potential"* (BRUNO, 2012, p. 349).

[4] Original: "*It is in this performative and proactive power that the danger of data mining and profiling lies*" (BRUNO, 2012, p. 349).

[5] Tradução: o que parece à primeira vista ser um jogo de soma zero é, na verdade, um conjunto de relações interdependentes (KERR & BARRIGAR, 2012, p. 386).

[6] Original: "[*c]onstructing an identity through the use of symbolic representations is a matter of information control*" (KERR & BARRIGAR, 2012, p. 386).

> *Harvard professor Lawrence Lessig called attention to the fact that the very architecture of the Internet, that is, the hardware and software that make it up with technical structure and codes governing its functioning, are also ways to regulate human behavior. According to professor Lessig, regulation through architecture is sometimes even more effective than other more familiar forms such as law, economics (market) and social norms. That's why he coined the well known phrase "Code is Law"(Lessig, 2000), since the very architecture of the sites makes us hostage of the algorithms, regulating our behavior as well as the law and creating serious obstacles to access to information, individual autonomy, privacy and freedom of expression (Lessig, 2006). The Internet is plastic and changeable and the fact that we are unwittingly becoming hostages of the algorithms that insert us on these bubbles, seeking the promise of hyperconnectivity and its facilities, has been seen as one of the most drastic changes, and subtle, because it is often unnoticeable. In a techno-regulated context ruled by algorithms' binary logic of "can/can't", the democratic potential of the connected public sphere and even the influence of the rule of law can be dramatically reduced* (MAGRANI, 2017, p. 8-9)[7].

Como consequência, vivemos em um mundo onde as identidades são facilmente manipuladas por atores com enorme concentração de poder, os quais, sem a devida regulação, têm a capacidade de modificar comportamentos e, portanto, decisões políticas. As eleições de Donald Trump nos Estados Unidos em 2016 e de Jair Bolsonaro no Brasil em 2018, então, são alguns dos casos em que o papel da tecnologia – em especial, das redes sociais – foi determinante para o exercício da democracia. Logo, o presente capítulo analisará como o capitalismo de vigilância vem impactando as relações sociais e políticas ao longo do século XXI no que diz respeito ao controle dos corpos e à reprodução de ideias e práticas enviesadas, ao papel das redes sociais e à concentração e domínio da informação e às consequências para a democracia.

---

[7] Tradução: O professor de Harvard Lawrence Lessig chamou atenção para o fato de que a própria arquitetura da Internet, ou seja, os *hardwares* e o *softwares* que a compõe com a estrutura técnica e os códigos que regem seu funcionamento, também são formas de regular o comportamento humano. Segundo o professor Lessig, a regulação por meio da arquitetura às vezes é ainda mais eficaz do que outras formas mais conhecidas, como o direito, a economia (mercado) e as normas sociais. Por isso cunhou a conhecida frase "Código é Lei" (Lessig, 2000), já que a própria arquitetura dos sites nos torna reféns dos algoritmos, regulando tanto nosso comportamento quanto a lei e criando sérios obstáculos ao acesso à informação, autonomia individual, privacidade e liberdade de expressão (Lessig, 2006).
A Internet é plástica e mutável e o fato de estarmos inadvertidamente nos tornando reféns dos algoritmos que nos inserem nessas bolhas, buscando a promessa da hiperconectividade e suas facilidades, tem sido visto como uma das mudanças mais drásticas, e sutis, porque muitas vezes é imperceptível. Em um contexto tecnorregulado regido pela lógica binária de algoritmos de "pode /não pode", o potencial democrático da esfera pública conectada e até mesmo a influência do estado de direito podem ser drasticamente reduzidos (MAGRANI, 2017, p. 8-9).

3.1 Biopoder e a questão do *bias*

Foucault (2007) define biopoder como o "poder sobre a vida e os corpos das espécies"; o que tem uma forte relação com a segurança, uma vez que esta lida com a regulação do trânsito dos corpos pelo espaço (FOUCAULT, 2007). No entanto, segundo Ayse Ceyhan (2012), esse poder não está restrito ao Estado: "*Indeed, in light of the current transformations occurring in the space of mobility as well as in the nature and the location of regulative powers, we witness a new modality of (bio)power*."[8] Conforme aumenta nossa dependência de tecnologias de informação e comunicação (TICs), o poder é modificado, se tornando mais híbrido e desterritorializado à medida que é exercido em centros de processamentos de dados e nos *headquarters* das *big tech,* além de estar cada vez mais disperso em meio ao cotidiano. Isto é, os reais detentores do poder atualmente são essas empresas que controlam as informações de bilhões de pessoas e as monitoram rotineiramente (CEYHAN, 2012, p. 38-40).

Trata-se de uma "nova modalidade de poder." O controle dos corpos não mais é exercido somente pelo Estado, que delimita como estes se deslocam dentro e fora do território. A nova assemblagem de vigilância (LYON, 2001) é marcada pelo "rastreamento de partes dos corpos (biometria) e comportamentos, assim como o escrutínio de seus projetos e pensamentos", viabilizados pelas tecnologias desenvolvidas pelas *big tech,* como os projetos do Google de mapeamento do genoma humano, evidenciando a presença da empresa em virtualmente todos os aspectos da vida, incluindo lazer, segurança e saúde (CEYHAN, 2012, p. 44-5, tradução minha[9]).

Portanto, a vigilância pode ser entendida como "uma tecnologia política de gestão populacional", que engloba "todos os aspectos da vida pública e privada dos indivíduos" conforme está presente "em tempo real e em termos de intenções e projetos futuros." Ceyhan argumenta que "os espaços de circulação e a natureza do

[8] Tradução: Com efeito, à luz das atuais transformações que ocorrem tanto no espaço da mobilidade como na natureza e na localização dos poderes reguladores, testemunhamos uma nova modalidade de (bio) poder (CEYHAN, 2012, p. 38).

[9] Original: "*As such contemporary biopower is hybrid. It opens new assemblages of technologies and techniques and is no longer processed by the sole control of populations through sexuality and health, but by the tracking of individuals' body parts (biometrics) and behaviors as well as the scrutiny of their projects and thoughts*" (CEYHAN, 2012, p. 45).

poder regulatório mudaram consideravelmente" uma vez que o virtual se torna um novo espaço de convivência e os locais de processamento e análise de dados ganham cada vez mais importância (CEYHAN, 2012, p. 40-4, tradução minha[10]).

"*Consequently, more than a straightforward biopolitical power of the subjugation of bodies, what we witness today resembles better the politics of artefacts, which, by its very design, includes certain interests and excludes others*"[11] (CEYHAN, 2012, p. 44). Tais artefatos, segundo Ceyhan, conectam diferentes tecnologias entre si, produzindo uma atmosfera de vigilância constante e descentralizando o poder das mãos do Estado, englobando também locais "não-tradicionais" como empresas de tecnologia e telefonia, lojas e a Internet. Como consequência, atores como o Google se tornaram as mais importantes ferramentas de vigilância biopolíticas, devido à coleta, processamento e análise de volumes monumentais de dados sobre os indivíduos.

Nesse processo, todavia, é importante lembrar que todas essas tecnologias são desenvolvidas por humanos: indivíduos carregados de ideias, concepções e experiências, que tendem a ser reproduzidas em suas invenções ainda que este não fosse o objetivo. Assim, decisões orientadas por dados podem impactar negativamente grupos historicamente marginalizados, enquanto outros são favorecidos, reforçando desigualdades (D'ALESSANDRO et al, 2017).

Um desses casos pode ser classificado como "*discrimination-in, discrimination-out*", onde (intencionalmente ou não) algum tipo de discriminação é inserido em um modelo de análise e este acaba reproduzindo-a (D'ALESSANDRO et al, 2017). Nesse sentido, podemos citar como exemplo as práticas de *profiling* orientadas por informações demográficas como endereço,

---

[10] Original: "*In this chapter surveillance is considered as a political technology of population management. (p. 40) Surveillance covers all aspects of the public and private life of individuals as they are implemented in the real-time and also in terms of future intentions and projects (p. 41) [T]he space of circulation and the nature of the regulative power have considerably changed. Not only has the space of mobility been extended outside the state borders and embraced the whole globe, but it has also become virtualized and open-ended with the display of a variety of technologies of information and communication as well as the development of huge databases where flows of information are processed and data mined*" (CEYHAN, 2012, p. 44).

[11] Tradução: Consequentemente, mais do que um poder biopolítico direto de subjugação dos corpos, o que testemunhamos hoje se assemelha melhor à política dos artefatos, que, por sua própria concepção, inclui certos interesses e exclui outros (CEYHAN, 2012, p. 44).

nível de escolaridade, renda, gênero e raça, privilegiando indivíduos com “melhores estatísticas.” Browne (2012) ilustra esse cenário com o ocorrido no registro para as eleições de 2000 nos Estados Unidos, quando no estado da Flórida alguns grupos foram classificados como “ilegítimos segundo linhas raciais”, privando "cerca de oito mil eleitores em potencial, muitos deles afro-americanos", de exercerem seu direito político (BROWNE, 2012, p. 76).

> Junto a outros indicativos sobre economia, violência, (necro)política e representação midiática, estes casos lembram que racismo “não deve ser entendido como um comportamento excepcional dos indivíduos desviando de uma norma social não-racista mas, diferentemente, como um sistema sociopolítico global” (ALI, 2013, p. 99) que inclui historicamente formatações dos campos produtivos da tecnologia que favorecem o treinamento enviesado de sistemas que intensificam discriminações e opressões. Os algoritmos são “idealizados por pessoas, e pessoas incorporam seus vieses inconscientes nos algoritmos. É raramente intencional – mas isso não significa que devemos ignorar a responsabilidade dos cientistas de dados. Significa que devemos ser críticos e vigilantes sobre as coisas que podem dar errado” (BROUSSARD, 2018, p.2891) (SILVA, 2020, p. 124).

Outro exemplo é “a característica de editorialização dos algoritmos e interfaces das plataformas como modo de gerar ou moldar informação e desinformação.” Enquanto, em 2014, os protestos do movimento “*Black Lives Matter*” nos Estados Unidos eram retratados com destaque nas redes sociais e na imprensa, o Facebook não fez nenhuma menção a este no seu recém-lançado “*Top Trends*”, pois o algoritmo concluiu que não se tratava de uma história “relevante.” Como consequência, “podemos falar de uma opacidade algorítmica que, por sua vez, decide visibilidade e invisibilidade de temas, levando ativistas e pesquisadores a uma dificuldade maior de identificar causas e efeitos” (SILVA, 2020, p. 132).

Nesse sentido, um outro tipo de *bias* perpetuado pela tecnologia está ligado a problemas de super e sub-representação: no primeiro caso, certos grupos tendem a ser favorecidos por constituírem uma maioria num espectro de análise, sendo melhor avaliados; enquanto no segundo, devido à baixa quantidade de amostras nesse mesmo cenário analítico, tendem a ser marginalizados, vistos como “pontos fora da curva” (D'ALESSANDRO et al, 2017). Como o trabalho “Vamos conversar, bancos de imagens?” do coletivo Desabafo Social mostra, palavras como “bebês” e “família” resultam majoritariamente em pessoas brancas, o que tende a reproduzir o racismo (SILVA, 2020, p. 132-3).

Ademais, como aponta Safiya Noble (2018), em resultados de busca de imagens, há uma tendência em plataformas como Google de reproduzir estereótipos nocivos de grupos minoritários como a hipersexualização de garotas negras e latinas. A autora afirma que "'na internet e nos nossos usos rotineiros da tecnologia, a discriminação está embutida nos códigos computacionais e, cada vez mais, em tecnologias de inteligência artificial das quais dependemos, por escolha ou não'" (SILVA, 2020, p. 132).

No ato de vigilância, ainda, é essencial levar em consideração o papel do gênero já que "ser vigiado" é uma noção extremamente "genderizada". Num ambiente onde o controle é orientado por informação, as pessoas são forçadas a viver em uma lógica de dois gêneros. Como consequência, "pessoas transgênero e transexuais devem se enquadrar em uma dessas categorias." Ademais, em cenários urbanos, o fenômeno da "genderização" é comumente visto conforme a maioria dos operadores de câmeras de segurança são homens, enquanto a maior parte dos corpos vigiados são mulheres, que tendem a ser o público que mais transita em locais onde essas câmeras estão presentes, como transporte público e centros comerciais (KOSKELA, 2012, p. 51-2, tradução minha[12]).

> *Heteronormative rules still regulate what can be revealed, and when. Constantly cautioned about dangerous unseen observers, women are advised to pay attention to their being-looked-at-ness, as if they are on constant display. Implicitly, women are criticized for straying from such rules of display: as if they should not "wear" the body they were born in. Such meanings reinforce the different ways that women are constructed as vulnerable. On one hand, surveillance equipment can be read as a sign of danger (distrust, need for control) and can thus amplify a sense of vulnerability. On the other hand, the promise of increased security generates a pressure for women to accept surveillance* (KOSKELA, 2012, p. 52-3)[13].

[12] Original: "*So, for example, in many urban settings surveillance is gendered at a very simple level: most people behind a surveillance camera are male and the people under surveillance are disproportionately female. More than men, women tend to occupy the spaces where surveillance cameras are present, such as shopping malls and public transport. At the same time, the professions responsible for conducting video surveillance, and acting on surveill images, are male dominated (p. 51). The gendered nature of surveillance also becomes apparent in situations in which one has to prove her/his (sic) identity. Information-based control forces people to confront the two-gendered world. In official contexts, transgender and transsexual people have to fit in either of these categories"* (KOSKELA, 2012, p. 52).

[13] Tradução: Regras heteronormativas ainda regulam o que pode ser revelado e quando. Constantemente advertidas sobre perigosos observadores invisíveis, as mulheres são aconselhadas a prestar atenção ao fato de serem observadas, como se estivessem em constante exibição. Implicitamente, as mulheres são criticadas por se desviarem de tais regras de exibição: como se não devessem "vestir" o corpo em que nasceram. Tais significados reforçam as diferentes maneiras pelas

"O amplo interesse, por diferentes partes, na captura e utilização de informações psíquicas e emocionais extraídas de nossos dados nas plataformas digitais alimentam hoje o que a pesquisadora Fernanda Bruno (2018) chamou de uma economia psíquica dos algoritmos" (Apud BENTES, 2019, p. 225). Isto é, ao traçar uma relação entre nossos dados psicossociais e emocionais e os padrões de nossas vidas cotidianas, os perfis individuais orientam a produção de previsões em larga escala aproximando personalidades semelhantes e viabilizando maior influência "sobre o comportamento tanto de um indivíduo específico quanto de seus similares" (BENTES, 2019, p. 225).

Assim, outro aspecto problemático da vigilância quanto ao controle dos corpos está ligado ao monitoramento das crianças no ambiente virtual. Segundo Valerie Steeves (2012), "[a]s experiências das crianças (...) fornecem um excelente contexto para mapear as formas contraditórias em que a vigilância é implementada como um princípio organizacional dentro dos espaços online" (2012, p. 359, tradução minha[14]). Pois, o ciclo de coleta, processamento e análise de dados do capitalismo de vigilância, infelizmente, também se aplica a crianças e adolescentes, fazendo com que estes sofram todo tipo de manipulação pelas *big tech*. Contudo, inclusive os pais são agentes de vigilância já que, como uma forma de "proteger as crianças de perigos online", eles são incentivados por *sites* como *Club Penguin* a vigiar o comportamento dos filhos (STEEVES, 2012, p. 352, tradução minha[15]).

Logo, iniciativas de treinamento em segurança para pais promovidas com frequência por empresas como Google e Microsoft, criam uma atmosfera de educação para vigilância infantil, que faz uso de medidas de controle comandadas por *software* como bloqueio de *sites* considerados perigosos e monitoramento de conversas, curtidas e postagens. Logo, quem realmente tem poder sobre as crianças são as empresas detentoras desses controles e dos espaços onde elas convivem.

---

quais as mulheres são construídas como vulneráveis. Por um lado, o equipamento de vigilância pode ser lido como um sinal de perigo (desconfiança, necessidade de controle) e pode, assim, amplificar uma sensação de vulnerabilidade. Por outro lado, a promessa de maior segurança gera uma pressão para que as mulheres aceitem a vigilância (KOSKELA, 2012, p. 52-3).

[14] Original: "*Children's experiences accordingly provide an excellent context in which to map the contradictory ways in which surveillance is implemented as an organizational principle within online spaces*" (STEEVES, 2012, p. 359).

[15] Original: "*Surveillance is expressly promoted on sites like Club Penguin as a way to protect children from online dangers, and parents are often co-opted into a joint surveillance project of care and control with benign corporate monitors"* (STEEVES, 2012, p. 352).

"*Unlike the panoptic gaze of parental control software, which seeks to encourage the child to internalize the watcher, corporate surveillance seeks to invisibly manipulate the child's identity play to privilege behaviors and identities that conform to the needs of the marketplace*"[16] (STEEVES, 2012, p. 356-7).

Nesse sentido, os mecanismos do capitalismo de vigilância buscam construir "uma 'arquitetura de decisões' (...), uma organização específica dos contextos nos quais as decisões são tomadas a fim de influenciar o comportamento em certa direção" (BENTES, 2019, p. 226). *Sites* como *Neopets, Club Penguin* e *Webkinz*, por exemplo, simulam uma realidade caracterizada por elementos comerciais como mercados de ações, oportunidades de emprego e uma indústria de serviços, onde os jogadores são incentivados a trabalhar e ganhar "dinheiro" a ser usado em produtos virtuais, fazendo com que aqueles com menos recursos sejam inferiorizados pelos demais. Portanto, "as crianças são incentivadas a acreditar que o objetivo do jogo e das interações sociais é adquirir bens de consumo", o que influencia como elas agem no mundo real, moldando seu comportamento em torno de uma lógica capitalista (STEEVES, 2012, p. 357, tradução minha[17]).

3.2 "O Dilema das Redes"

A rapidez com que as redes sociais foram incorporadas ao nosso cotidiano é espantosa. Mais rápido do que o rádio, o cinema, a televisão, ou até mesmo a Internet, esse meio de comunicação mudou completamente a forma como diversas sociedades interagem entre si e consomem entretenimento e informações. Um dos casos mais emblemáticos desse fenômeno é o Facebook, dono de 3 dos 4 maiores aplicativos de comunicação: "o WhatsApp e o Messenger, com 1,2 bilhão de usuários, [e] o Instagram, com 700 milhões", tornando a empresa uma das mais valiosas do mundo, mas também uma das mais poderosas (LANCHESTER, 2017).

[16] Tradução: Ao contrário do olhar panóptico do software de controle parental, que busca encorajar a criança a internalizar o observador, a vigilância corporativa busca manipular invisivelmente a brincadeira de identidade da criança para privilegiar comportamentos e identidades que estejam em conformidade com as necessidades do mercado (STEEVES, 2012, p. 356-7).

[17] Original: "*Since these virtual worlds are instructive, teaching children models for being and experiencing the world, they encourage children to believe that the objective of play and social interaction is to acquire consumer goods*" (STEEVES, 2012, p. 357).

Conforme se consolidaram, as empresas donas das redes sociais promoveram um agravamento na relação entre vigilância e liberdades civis. Enquanto mobilizadoras, as redes sociais tiveram um papel importante no movimento da "Primavera Árabe", por exemplo, fomentando a expressão política numa "onda de movimentos democráticos" no Norte da África e Oriente Médio em 2011. Por outro lado, porém, a popularização das redes implica no consentimento de mecanismos de invasão de privacidade, na concessão voluntária de informações pessoais, na corroboração com a vigilância do nosso comportamento *online* (ABU-LABAN, 2012, p. 421) e *offline* (LANCHESTER, 2017).

Ademais, nossa atenção vem sendo disputada por esses mecanismos de forma a nos manter engajados o maior tempo possível, o que permite a criação de perfis mais acurados por parte do capitalismo de vigilância, garantindo maiores lucros, mas também aumentando nossa participação na plataforma: quanto mais se sabe sobre o usuário, mais certeza se tem sobre a probabilidade de ele clicar em uma propaganda, aumentando o valor a ser cobrado por esta, assim como a participação do usuário.

"No cerne desta disputa econômica pela atenção, as empresas de tecnologia requerem de seus usuários que o uso de seus serviços não seja apenas um comportamento pontual, mas que se torne um hábito." Em geral, "os países que mais passam tempo conectados gastam uma média de 8 horas por dia na internet"; entre estes está o Brasil, com "uma média diária de 8h56min de conexão, sendo cerca de 4h59min em computadores, 3h56min em celulares e 3h43min em redes sociais" (BENTES, 2019, p. 228-32).

Ao passarmos tanto tempo conectados, segundo Yael Eisenstat (2020), as redes sociais inflamam cada vez mais nossas "bolhas sociais", pois o que vemos é altamente selecionado de acordo com nossos perfis, acentuando as polaridades de ideias:

> *We are being manipulated by the current information ecosystem entrenching so many of us so far into absolutism that compromise has become a dirty word. Because right now, social media companies like Facebook profit off of segmenting us and feeding us personalized content that both validates and exploits our biases. Their bottom line depends on provoking a strong emotion to keep us engaged, often incentivizing the most*

> *inflammatory and polarizing voices, to the point where finding common ground no longer feels possible* (EISENSTAT, 2020)[18].

Se tudo que vemos nas redes é arquitetado para espelhar nossos pensamentos, vontades e ideias, quando vemos algo que foge disso, nos opomos radicalmente, julgamos ser mentira ou simplesmente irreal. Os *mindsets* ideológicos estão tão rígidos que discordar de alguém é visto como uma condenação pessoal (EISENSTAT, 2020). Contudo, a base da democracia moderna está na pluralidade de ideias (SARTORI, 1994). Se não pudermos ter debates saudáveis, qual será o futuro da política?

Um agravante desse cenário, então, são as redes sociais, que encorajam esse tipo de comportamento; afinal, isso garante mais tempo do usuário engajado na plataforma. Infelizmente, mentiras são mais interessantes do que a verdade (EISENSTAT, 2020). Alguns exemplos retratados no documentário *O dilema das redes* (2020) são a popularização do movimento "terraplanista" e o episódio "Pizzagate", ambos iniciados como inverdades disseminadas *online* e direcionadas para pessoas com perfis tendenciosos a acreditar e corroborar com teorias conspiratórias.

Acredita-se que existam duas grandes motivações para fomentar *fake news*. Uma é monetária, geralmente histórias onde os autores são revelados e que buscam receber mais atenção nas redes sociais, para, com isso, lucrar com a receita da publicidade. Outra motivação é ideológica, favorecendo um grupo político sem necessariamente se identificar, como o caso de *sites* fabricados no Leste Europeu em favor de Donald Trump à época das eleições de 2016 (ALLCOTT & GETZHOW, 2017, p. 217).

As redes sociais, então, são um espaço próspero para as *fake news* devido aos baixos custos de ingresso e veiculação da informação, à dificuldade de identificar uma notícia como falsa já que os conteúdos são padronizados e à

[18] Tradução: Estamos sendo manipulados pelo atual ecossistema de informações que está entrincheirando tantos de nós até agora no absolutismo que o compromisso se tornou um palavrão. Porque agora, empresas de mídia social como o Facebook lucram com a segmentação e nos fornecendo conteúdo personalizado que valida e explora nossos preconceitos. Seu resultado final depende de provocar uma emoção forte para nos manter engajados, muitas vezes incentivando as vozes mais inflamatórias e polarizadoras, a ponto de encontrar um terreno comum não parecer mais possível (EISENSTAT, 2020).

facilidade de engajar com um conteúdo direcionado. Como consequência, aqueles que acreditam em notícias falsas têm suas crenças menos precisas, questionando a legitimidade de informações verdadeiras, o que dificulta a distinção entre as informações. Ademais, conforme mais pessoas acreditam em notícias fabricadas, menores são os incentivos econômicos para produzir pesquisas precisas (ALLCOTT & GETZHOW, 2017, p. 219-21).

As soluções para esse problema, felizmente, podem ser facilmente implementadas: o Facebook, por exemplo, poderia parar de incentivar esse tipo de comportamento, revisando o conteúdo publicado antes de recomendá-lo para outros usuários e viralizá-lo; e deixando de amplificar grupos de ódio e teorias da conspiração (EISENSTAT, 2020). Todavia, a regulação presente e o atual modelo econômico – em que a desinformação é tão lucrativa – não promovem os incentivos necessários para isso. Na verdade, o cenário econômico-legal protege essas empresas e seu comportamento predatório (DILEMA DAS REDES, 2020).

A título de exemplo, o Facebook recentemente ameaçou bloquear usuários na Austrália de compartilhar notícias no Instagram e Facebook caso uma lei que "força gigantes da tecnologia a pagar a editoras para distribuir partes de seu conteúdo" seja aprovada. Segundo a empresa, a lei prejudicaria mais as editoras do que a si; o diretor da empresa na Austrália e Nova Zelândia, Will Eason, afirmou que a legislação "'mal compreende a dinâmica da internet e prejudicará as próprias organizações de notícias que o governo está tentando proteger.'" Caso a proposta australiana seja adotada, espera-se que este se torne um modelo mais disseminado ao redor do mundo, o que representaria um grande estímulo à imprensa, especialmente para noticiários locais, que vem perdendo cada vez mais investimento (FISCHER, 2020, tradução minha[19]).

A resposta do Facebook, no entanto, é bastante representativa de um padrão por parte das *tech giants*, que frequentemente ameaçam tirar seu serviço inteiramente de um país quando têm suas ambições freadas por medidas

[19] Original: *"Facebook said Monday that it will block users in Australia from sharing news on Facebook and Instagram if a controversial law forcing tech giants like Facebook and rival Google to pay publishers to distribute portions of their content passes this fall. (...) In a blog post Monday, Will Eason, Facebook's managing director for Australia & New Zealand, writes that the legislation 'misunderstands the dynamics of the internet and will do damage to the very news organizations the government is trying to protect*.'" (FISCHER, 2020).

regulatórias. Na União Europeia, uma medida semelhante foi proposta de modo que os países-membro teriam de adotar leis que forçassem essas empresas a pagar veículos de notícias. O Google, então, ameaçou tirar o *Google News* caso os países-membro seguissem em frente com a medida, e, em 2014, o recurso foi retirado da Espanha (FISCHER, 2020).

Além da disseminação de notícias falsas, plataformas como Google e Facebook divulgam conteúdos sensíveis como nudez infantil, discursos de ódio, conteúdo extremista e terrorista. E novamente, os esforços para conter o compartilhamento desses é mínimo; exceto no que diz respeito ao conteúdo sexual, que, no caso do Facebook, é tratado com extremo rigor (LANCHESTER, 2017).

> A escala de prioridades é bizarra, e só faz sentido no contexto americano, em que a mais ligeira sugestão de sexualidade explícita é logo tingida de impureza moral. Mesmo fotos de mulheres amamentando seus filhos são banidas e eliminadas num átimo. Já mentiras e mera propaganda podem circular à vontade. Para entender esse quadro, basta adotar o ponto de vista dos anunciantes: nenhum deles quer aparecer ao lado de uma foto de seios nus, pois isso pode prejudicar sua marca; mas não se incomodam em aparecer ao lado de mentiras, porque essas mentiras podem inclusive ajudá-los a encontrar os consumidores aos quais pretendem direcionar seus anúncios (LANCHESTER, 2017).

Comumente, as detentoras das redes sociais argumentam que não é seu dever regular o conteúdo em suas plataformas, pois isso iria inibir a liberdade de expressão dos usuários. Porém, após os protestos por supremacistas brancos e grupos antirracismo em Charlottesville, empresas como Facebook anunciaram que iriam fortalecer o monitoramento de discursos de ódio (ANGWIN et al, 2017).

Contudo, pouco foi feito quanto à revisão da plataforma de compra de anúncios. Como divulgado na reportagem "*Facebook Enabled Advertisers to Reach 'Jew Haters'*" da ProPublica (ANGWIN et al, 2017), ao tentar publicar um anúncio direcionado a categoria "*jew hater*", descobriu-se que a categoria com pouco mais de 2 mil pessoas era muito limitada para prosseguir com o pedido. Então, foi automaticamente sugerida a categoria "*Second Amendment*" para atingir um público maior, cerca de 119 mil pessoas, "presumivelmente porque seu sistema

correlacionou entusiastas de armas com antissemitas" (ANGWIN et al, 2017, tradução minha[20]).

> *In all likelihood, the ad categories that we spotted were automatically generated because people had listed those anti-Semitic themes on their Facebook profiles as an interest, an employer or a "field of study." Facebook's algorithm automatically transforms people's declared interests into advertising categories* (ANGWIN et al, 2017)[21].

De forma semelhante, uma reportagem conduzida pelo BuzzFeed News (KANTROWITZ, 2017) para analisar o sistema de anúncio do Google observou que a plataforma permite direcionar propagandas para pessoas que buscam termos racistas:

> *Type 'White people ruin,' as a potential advertising keyword into Google's ad platform, and Google will suggest you run ads next to searches including 'black people ruin neighborhoods.' Type 'Why do Jews ruin everything,' and Google will suggest you run ads next to searches including 'the evil jew' and 'jewish control of banks.' (...) Following our inquiry, Google disabled every keyword in this ad campaign save one — an exact match for 'blacks destroy everything,' is still eligible. Google told BuzzFeed News that just because a phrase is eligible does not guarantee an ad campaign will run against it. A total of 17 ad impressions were served before the keywords were disabled* (KANTROWITZ, 2017)[22].

Enquanto no sistema do Facebook são selecionadas categorias de um catálogo elaborado a partir de informações dos usuários como interesses, localização e gênero, no Google, os anúncios são direcionados segundo termos que se espera serem procurados pelos usuários, o que confere uma maior incerteza ao seu sistema (KANTROWITZ, 2017).

---

[20] Original: "*Facebook's automated system suggested 'Second Amendment' as an additional category that would boost our audience size to 119,000 people, presumably because its system had correlated gun enthusiasts with anti-Semites*" (ANGWIN et al, 2017).

[21]Tradução: Muito provavelmente, as categorias de anúncios que vimos foram geradas automaticamente porque as pessoas listaram esses assuntos antissemitas em seus perfis do Facebook como um interesse, um empregador ou um "campo de estudo." O algoritmo do Facebook transforma automaticamente os interesses declarados das pessoas em categorias de publicidade (ANGWIN et al, 2017).

[22]Tradução: Digite "ruína dos brancas" como uma possível palavra-chave de publicidade na plataforma de anúncios do Google, e o Google irá sugerir que você exiba anúncios ao lado de pesquisas incluindo "negros arruinam bairros". Digite "Por que os judeus arruínam tudo" e o Google irá sugerir que você execute anúncios ao lado de pesquisas, incluindo "o judeu do mal" e "controle judaico de bancos". (...) Seguindo nossa consulta, o Google desativou todas as palavras-chave nesta campanha publicitária, exceto uma - uma correspondência exata para "negros destroem tudo" ainda está qualificada. O Google disse ao BuzzFeed News que só porque uma frase é elegível não garante que uma campanha publicitária será executada contra ela. Um total de 17 impressões de anúncios foram veiculados antes de as palavras-chave serem desativadas (KANTROWITZ, 2017).

Segundo Evgeny Morozov (2013), a noção de que a globalização proporcionaria uma maior emancipação individual devido à disseminação de informação provavelmente foi uma alucinação prolongada dos anos 1990. O autor argumenta que tanto o capitalismo quanto o setor público facilmente se adaptaram ao regime digital, pois ambos prosperam em fluxos mais livres de informação. Isto é, há uma convergência entre os interesses políticos do setor público e os interesses comerciais das empresas de tecnologia uma vez que ambos se beneficiam da coleta e análise de dados em grande escala. Enquanto o setor privado está preocupado em aumentar suas taxas de lucro, as agências governamentais empregam esses dados de diversas maneiras: desde assuntos de segurança como combate ao terrorismo (como abordado previamente no capítulo anterior), até questões de coleta de impostos, como é o caso do governo italiano que faz uso do *redditometro*, uma ferramenta capaz de analisar os gastos de uma pessoa e comparar com sua renda para identificar possíveis fraudes (MOROZOV, 2013). Como consequência, a política passa a ser exercida para além dos espaços públicos:

> *Here's what that deficit would look like: the new digital infrastructure, thriving as it does on real-time data contributed by citizens, allows the technocrats to take politics, with all its noise, friction, and discontent, out of the political process. It replaces the messy stuff of coalition building, bargaining, and deliberation with the cleanliness and efficiency of data-powered administration.*
> *This phenomenon has a meme-friendly name: 'algorithmic regulation,' as Silicon Valley publisher Tim O'Reilly calls it. In essence, information-rich democracies have reached a point where they want to try to solve public problems without having to explain or justify themselves to citizens. Instead, they can simply appeal to our own self-interest—and they know enough about us to engineer a perfect, highly personalized, irresistible nudge* (MOROZOV, 2013)[23].

Portanto, nossa privacidade está em risco, devido à coleta predatória de dados pessoais por parte dos governos e das empresas de tecnologia e, consequentemente, à normalização da assemblagem de vigilância, classificada por Morozov como o "arame farpado invisível" (*"invisible barbed wire*") em torno de

[23] Tradução: É assim que esse déficit seria: a nova infraestrutura digital, que prospera com base em dados em tempo real fornecidos pelos cidadãos, permite que os tecnocratas tirem a política, com todo o seu barulho, atrito e descontentamento, do processo político. Ele substitui a bagunça de construção, negociação e deliberação de coalizões pela limpeza e eficiência da administração baseada em dados. Este fenômeno tem um nome amigável ao meme: 'regulação algorítmica', como o editor do Vale do Silício Tim O'Reilly o chama. Em essência, as democracias ricas em informações chegaram a um ponto em que desejam tentar resolver os problemas públicos sem ter que se explicar ou se justificar aos cidadãos. Em vez disso, eles podem simplesmente apelar para o nosso próprio interesse - e eles sabem o suficiente sobre nós para criar um empurrão perfeito, altamente personalizado e irresistível (MOROZOV, 2013).

nossas vidas sociais e intelectuais. O "*Big data*, com seus muitos bancos de dados interconectados que se alimentam de informações e algoritmos de proveniência duvidosa, impõe severas restrições sobre como amadurecemos política e socialmente" (MOROZOV, 2013, tradução minha[24]). Com a vigilância tão perpetuada pelo modelo econômico, mas também pelos modos de governo atuais, esta é naturalizada no nosso dia a dia de tal forma que vivemos na ilusão de que somos livres para fazermos e irmos onde desejarmos, quando na verdade, nossos passos e pensamentos estão sendo manipulados por terceiros (MOROZOV, 2013).

"*The more information we reveal about ourselves, the denser but more invisible this barbed wire becomes. We gradually lose our capacity to reason and debate; we no longer understand why things happen to us*"[25] (MOROZOV, 2013). Para o autor, então, nossa única saída é a privacidade, pois esta seria a única maneira de nos vermos presos por esse arame e, potencialmente, nos libertarmos (MOROZOV, 2013).

3.3 A Informação e o Declínio da Democracia

De acordo com Shoshana Zuboff (2019), no capitalismo de vigilância, "*freedom and ignorance are no longer twin born, no longer two sides of the same coin called mystery*"[26] (p. 466). Na verdade, há atualmente uma convergência nunca antes vista entre liberdade e conhecimento: enquanto os membros desse novo modelo econômico reivindicam a liberdade de ordenar o conhecimento, usando-o como uma forma de proteger e expandir tal liberdade, sua acumulação irrestrita de poder institui uma lógica de inclusão-exclusão devido ao controle da informação na sociedade (ZUBOFF, 2019).

---

[24]Original: "*Big data, with its many interconnected databases that feed on information and algorithms of dubious provenance, imposes severe constraints on how we mature politically and socially*" (MOROZOV, 2013).

[25]Tradução: Quanto mais informações revelamos sobre nós mesmos, mais denso, porém mais invisível, esse arame farpado se torna. Gradualmente perdemos nossa capacidade de raciocinar e debater; não entendemos mais porque as coisas acontecem conosco (MOROZOV, 2013).

[26]Tradução: liberdade e ignorância não são mais gêmeos, não mais dois lados da mesma moeda chamada mistério (ZUBOFF, 2019, p 466).

Isto é, a articulação entre conhecimento e liberdade leva a um aumento da assimetria de poder devido ao controle da divisão do aprendizado na sociedade por parte do capitalismo de vigilância: uma vez que grande parte da informação que acessamos é organizada pelas *big tech*, estas controlam a maneira como conhecemos e, nesse processo, nos conhecem. "*This cycle will be broken only when we acknowledge as citizens, as societies, and indeed as a civilization that surveillance capitalists know too much to qualify for freedom*"[27] (ZUBOFF, 2019, p. 466-7).

A forma como acessamos o mundo se tornou digitalizada e mediada por terceiros, que, semelhante a um bibliotecário, controlam o que conhecemos. Nesse sentido, o mecanismo de busca do Google, enquanto um tipo de algoritmo, governa a biblioteca digital que é a *web* por meio de seleções e arranjos automatizados "pensados" de acordo com o perfil do usuário. Portanto, pessoas diferentes têm resultados e, consequentemente, conhecimentos diferentes (VAN OTTERLO, 2016, p. 50-6).

"*The idea is simple, yet very powerful: given a prediction model of individual behaviour, a company or government can exploit that model to manipulate the behaviour of large groups of individuals*"[28] (VAN OTTERLO, 2016, p. 59). Assim, um dos grandes problemas desse modelo é seu caráter oculto: não se sabe exatamente como os resultados são produzidos e elencados, e mesmo se a "receita" fosse revelada, a quantidade de dados e informações "excederia a capacidade humana de leitura e compreensão, uma vez que depende de vastos processos de coleta de informações, análise estatística, aprendizagem, amostragem e filtragem" (VAN OTTERLO, 2016, p. 72, tradução minha[29]). Sabe-se, no entanto, que esses mecanismos são orientados em parte por metodologias das Ciências Sociais. Então, para criar hierarquias de relevância, o capitalismo de vigilância

---

[27] Tradução: Este ciclo será quebrado apenas quando reconhecermos como cidadãos, como sociedades e, na verdade, como uma civilização que os capitalistas de vigilância sabem demais para se qualificar como liberdade (ZUBOFF, 2019, p. 466-7).

[28] Tradução: A ideia é simples, mas muito poderosa: dado um modelo de previsão do comportamento individual, uma empresa ou governo pode explorar esse modelo para manipular o comportamento de grandes grupos de indivíduos (VAN OTTERLO, 2016, p. 59).

[29] Original: "*Even if search algorithms were to report all of the decisions and information that determined the search results, it would exceed the capacity for human reading and comprehension, since it depends on vast processes of information gathering, statistical analysis, learning, sampling and filtering*" (VAN OTTERLO, 2016, p. 72).

reapropria métodos de pesquisa, assim como filosofias políticas, moldando a forma como vemos o mundo (BIRKBAK & CARLSEN, 2016, p. 38).

Segundo Andreas Birkbak e Hjalmar Bang Carlsen (2016), ao realizar, então, seu sonho originário de "organizar a informação do mundo" (WU, 2012), o Google se baseia na ideia de que a democracia funciona na *web*. O ordenamento de resultados (intitulado *PageRank*) age como uma espécie de eleição conforme a quantidade de "votos" do *site*: aqueles com mais visualizações e mais "credibilidade" – geralmente, mais antigos – tendem a aparecer entre os primeiros resultados, sendo mais favorecidos pelo algoritmo, conferindo um cenário de "tirania da maioria." Pois, se os *sites* "eleitos" pelo Google são os que primeiro aparecem na lista de resultados, estes continuam no poder, oferecendo pouco espaço para que outros se destaquem (BIRKBAK & CARLSEN, 2016, p. 42-3).

Como aponta Renée Diresta (2020), então, "[*p]ervasive generated text has the potential to warp our social communication ecosystem: algorithmically generated content receives algorithmically generated responses, which feeds into algorithmically mediated curation systems that surface information based on engagement.*"[30] Uma das maiores consequências, portanto, do ordenamento de informação controlada por algoritmos é a possibilidade de resultados manipulados receberem destaque como se fossem legítimos. Isto é, se um *site* é criado com o objetivo de espalhar notícias falsas mas ao mesmo tempo é reconhecido pelos mecanismos de *ranking* de resultados como verídico, este não só é acessado por diversas pessoas como também pode ser consumido como verdade (DIRESTA, 2020).

Como mostra Diresta (2019), as *fake news*, na verdade, começaram como notícias falsas inventadas e compartilhadas por pessoas com motivações políticas ou econômicas. Os resultados, especialmente quanto à eleição de Donald Trump, ainda estão sendo discutidos (DIRESTA, 2019), porém, o fato é que com o avanço da tecnologia está cada vez mais difícil detectar tais mentiras. Por exemplo, recentemente introduzido, o *Generative Pre-training Transformer 3* (GPT-3) é um

[30] Tradução: Texto gerado universalmente tem o potencial de distorcer nosso ecossistema de comunicação social: o conteúdo gerado por algoritmos recebe respostas geradas por algoritmos, que alimentam sistemas de curadoria mediados por algoritmos que revelam informações com base no engajamento (DIRESTA, 2020).

modelo de linguagem altamente sofisticado capaz de produzir frases humanizadas que, se usado maliciosamente, pode viabilizar a produção de "*deep fakes*": uma categoria de *fake news* que dificilmente pode ser verificada, provocando sérias consequências sobre a maneira como o conteúdo digital é produzido e reproduzido Como consequência, corre-se o risco de, sabendo das chances de algo ser falso, políticos ignorarem acusações reais comprovadas por registros de áudio ou vídeo, taxando-as de *deep fake* (DIRESTA, 2020).

> *As anyone who has followed a heated Twitter hashtag can attest, activists and marketers alike recognize the value of dominating what's known as "share of voice": Seeing a lot of people express the same point of view, often at the same time or in the same place, can convince observers that everyone feels a certain way, regardless of whether the people speaking are truly representative—or even real. In psychology, this is called the majority illusion. As the time and effort required to produce commentary drops, it will be possible to produce vast quantities of AI-generated content on any topic imaginable. Indeed, it's possible that we'll soon have algorithms reading the web, forming "opinions," and then publishing their own responses. This boundless corpus of new content and comments, largely manufactured by machines, might then be processed by other machines, leading to a feedback loop that would significantly alter our information ecosystem. (...) In the future, deepfake videos and audiofakes may well be used to create distinct, sensational moments that commandeer a press cycle, or to distract from some other, more organic scandal. But undetectable textfakes—masked as regular chatter on Twitter, Facebook, Reddit, and the like—have the potential to be far more subtle, far more prevalent, and far more sinister. The ability to manufacture a majority opinion, or create a fake-commenter arms race—with minimal potential for detection—would enable sophisticated, extensive influence campaigns* (DIRESTA, 2020)[31].

[31] Tradução: Como qualquer pessoa que tenha seguido uma hashtag acalorada do Twitter pode atestar, ativistas e profissionais de marketing reconhecem o valor de dominar o que é conhecido como "*share of voice*": ver muitas pessoas expressando o mesmo ponto de vista, muitas vezes ao mesmo tempo ou mesmo lugar, pode convencer os observadores de que todos se sentem de uma determinada maneira, independentemente de as pessoas que falam serem verdadeiramente representativas - ou mesmo reais. Em psicologia, isso é chamado de ilusão da maioria. À medida que diminui o tempo e o esforço necessários para produzir comentários, será possível produzir grandes quantidades de conteúdo gerado por IA sobre qualquer tópico imaginável. Na verdade, é possível que em breve teremos algoritmos lendo a web, formando "opiniões" e publicando suas próprias respostas. Esse corpus ilimitado de novos conteúdos e comentários, em grande parte fabricado por máquinas, pode então ser processado por outras máquinas, levando a um ciclo de feedback que alteraria significativamente nosso ecossistema de informações.
(…) No futuro, vídeos e áudios *deepfake* podem muito bem ser usados para criar momentos distintos e sensacionais que comandam um ciclo de imprensa, ou para desviar a atenção de algum outro escândalo mais orgânico. Mas *textfakes* indetectáveis - mascarados como conversas regulares no Twitter, Facebook, Reddit e similares - têm o potencial de ser muito mais sutis, muito mais prevalentes e muito mais sinistros. A capacidade de fabricar uma opinião majoritária ou criar uma corrida armamentista de falsos comentadores - com potencial mínimo de detecção - permitiria campanhas de influência sofisticadas e extensas (DIRESTA, 2020).

As redes sociais, então, foram "determinante[s] para o rebaixamento do debate público, permitindo com mais facilidade a circulação das 'grandes mentiras' (*Große Lügen*) de que Hitler falava com entusiasmo – dessa vez transmitidas para um público gigantesco." E sem a devida regulação, esse cenário tende a continuar se perpetuando no futuro. Uma possibilidade para frear as *tech giants* seria enquadrá-las como uma forma de monopólio. Porém, nos Estados Unidos, o posicionamento quanto à lei antitruste é lido a partir de uma lógica de preços. Ao entender que "a queda dos preços indica que o mercado está funcionando, e que medida nenhuma é necessária contra o monopólio", nada pode ser feito quanto ao Facebook ou a Amazon, por exemplo, que "jamais foi incomodada pelas autoridades reguladoras, apesar da posição claramente monopolista que ocupa no mundo das vendas online a varejo, em especial de livros" (LANCHERSTER, 2017).

Ademais, junto às *fake news*, emergiu um novo grupo político potencialmente perigoso. Segundo Edward Leavy (2018), "tecnopopulismo se refere ao uso crescente de tecnologias digitais para coordenar ações e decisões coletivas em nome do chamado povo comum." Nesse sentido, partidos "tecnopopulistas" engajam com seus membros por meio da internet e "então alegam que suas ações são expressões diretas do que o público deseja." "Em contraste à forma como essas decisões são historicamente tomadas por membros do partido fora da vista do público, os resultados dos referendos *online* são saudados como expressando a 'vontade geral' do povo em um estilo significativamente diferente da política representativa convencional" (LEAVY, 2018, p. 2, tradução minha[32]).

São inaugurados, assim, partidos políticos "hibridizados" que dizem conceder parte do poder a seus membros. Devido ao seu caráter virtual, tais movimentos são mais suscetíveis ao público mais jovem, que tem mais facilidade de compreender como a política, assim como vários outros aspectos da vida em sociedade, podem ser digitalizados. Além disso, com as taxas de desemprego mais

[32] Original: "*The term technopopulism refers to the rising use of digital technology to coordinate collective action and decisions on behalf of the so-called common people. Technopopulist parties use the internet to engage their party members and then claim that their actions are direct expressions of what the public desires. (...) In contrast to the way these decisions are historically made by party insiders outside of public view, the results of online referenda are hailed as expressing the 'general will' of the people in a markedly different style than conventional representative politics*" (LEAVY, 2018, p. 2).

altas entre os jovens (cerca de 44,1% na Espanha e 36,9% na Itália), estes procuram novos meios de reinventar a política a seu favor. São exemplos desse fenômeno, os movimentos "*Podemos*" e "*Movimento Cinque Stelle*" (M5S), os quais usam as "redes sociais para direcionar os manifestantes antiausteridade em um partido convencional" e "organizar um movimento de protesto próprio", respectivamente (LEAVY, 2018, p. 32-5, tradução minha[33]).

Atualmente, então, o modelo político dominante está em risco de colapsar devido ao papel da informação sobre a verificação de consenso. Segundo o professor Renato Lessa (2012), a democracia nasce não com o propósito de representar, mas como uma forma de "deliberação coletiva a respeito de questões de interesse público", uma forma de autogoverno, que ao longo do tempo evolui para ser o "direito irrestrito de escolher quem nos governa", evidenciando o "esquema da representação" como fora definido por James Madison (LESSA, 2012).

Assim, ao abandonar o sentido grego de democracia no qual todos decidem por todos, a sociedade moderna adota uma nova forma de governo em que alguns são escolhidos para decidir por todos. Nesse sentido, vale ressaltar que, segundo Giovanni Sartori (1994), a divisão entre governantes e governados é pouco precisa, podendo ser definida principalmente pelo momento da eleição: momento de verificação de consenso em que o povo é chamado a governar ao escolher seus representantes. Ou seja, a democracia é definida pela distribuição do poder nas mãos do povo, que, ao votar em seus representantes, se faz ouvido e manifesta suas vontades (SARTORI, 1994).

Ademais, tanto Sartori quanto Lessa destacam a impossibilidade do autogoverno na democracia moderna. "Democracia é um sistema onde ninguém pode escolher a si mesmo, ninguém pode investir a si mesmo com o poder de governar e, por conseguinte, ninguém pode arrogar-se um poder incondicional e ilimitado" (SARTORI, 1994, p. 278), o que se deve segundo Lessa à inovação imaterial dos norte-americanos: um novo sistema político marcado pela teoria

[33] Original: "*Podemos has used social media to channel the energy of antiausterity protesters into a conventional party while the Five Star Movement used the internet to organize a protest movement of their own*" (LEAVY, 2018, p. 32).

contemporânea representativa, que entende a democracia como uma república em um pequeno território onde os cidadãos se autogovernam. Isto é, o Federalismo inaugura a implementação de um filtro entre população e governantes, levando a um modelo híbrido entre a democracia onde todos decidem por todos – sendo esta marcada pela manifestação de interesses privados - e o absolutismo onde um decide por todos – neste caso, caracterizado pela manifestação de interesses de cunho pessoal (LESSA, 2012).

Nesse sentido, o nível de informação disponível durante o processo decisório é essencial para a democracia; de forma que quando a população se una para eleger seu representante, então, os melhores sejam selecionados, e, estes "incentivados" a pensar no coletivo que representam, além de seus interesses particulares (LESSA, 2012). Portanto, para que haja produção de consenso, a população deve ter conhecimento sobre os diversos candidatos, suas propostas e posicionamentos, quais as condições em que o voto se dará; em suma, é preciso que as informações sobre os processos políticos sejam conhecidas pelos eleitores, fenômeno que Sartori denomina de "consenso procedimental" (SARTORI, 1994).

Segundo o autor, para que a democracia seja efetivamente posta em prática, quaisquer discordâncias devem ocorrer dentro das definições procedimentais compartilhadas. Não se trata, porém, sobre diversidade de ideias. O ponto principal é que, dentro de um conjunto de regras predeterminado, todos possam concordar ou discordar sobre certos temas, o que não diz respeito a conflitos de ideias, mas sim a pluralismo (SARTORI, 1994).

Diferente dos regimes autoritários, a democracia está baseada na "incerteza condicional". Enquanto no autoritarismo todos os aspectos da vida são sabidos e/ou controlados pelo Estado, sendo, portanto, "quase certo que os resultados políticos não incluem os resultados contrários aos interesses do aparato de poder", em regimes democráticos "não existe grupo cujos interesses possam excluir aprioristicamente consequências políticas com uma margem razoável de certeza" (PRZEWORSKI, 1984, p. 37).

Isto é, nas democracias a incerteza dos resultados eleitorais é institucionalizada: dentro de um conjunto de regras compartilhado por todos os

eleitores, o poder é distribuído entre o povo para que este determine quem os deve representar:

> As soluções para o problema da democratização residem nas instituições. Uma vez que esta afirmação pode soar inócua, é preciso enfatizar que ela exclui a possibilidade de a democracia ser o resultado de um compromisso baseado exclusivamente em questões substantivas. A democracia é possível quando as forças políticas relevantes conseguem encontrar instituições que garantam, com razoável margem de segurança, que seus interesses não serão afetados de modo considerável no decorrer da competição democrática. Mesmo não sendo o resultado exclusivo de um compromisso substantivo, a democracia pode ser o resultado de um compromisso institucional (PRZEWORSKI, 1984, p. 38).

Isto posto, o nível de informação disponível a cada um tem uma forte ligação com a formulação de opinião, o que, por sua vez orienta o voto. E, ao pensarmos atualmente no papel da tecnologia nesse processo, encontramos uma série de problemas, um deles sendo o constante monitoramento do nosso comportamento por parte de grandes empresas de tecnologia.

> *This problem is one of the defining threats of our generation. Influence operations exploit divisions in our society using vulnerabilities in our information ecosystem. They take advantage of our commitment to freedom of speech and the free flow of ideas. The social media platforms cannot, and should not, be the sole defenders of democracy and public discourse* (DIRESTA, 2018)[34].

A degradação da vontade individual é uma característica própria do capitalismo de vigilância, o qual, ao cooptar nossa atenção, viabiliza fenômenos como Trump, que sabe como chamar a atenção para si e explorar indignação. Segundo Lewis (2017), "'[s]e a política é uma expressão de nossa vontade humana, em níveis individuais e coletivos, então a economia da atenção está minando diretamente os pressupostos em que se baseia a democracia.'" Se Facebook e Google estão "gradualmente destruindo nossa capacidade de controlar nossas próprias mentes, poderia chegar um ponto, eu pergunto, em que a democracia não funcione mais?" (LEWIS, 2017, tradução minha[35]).

---

[34] Tradução: Este problema é uma das ameaças definidoras de nossa geração. As operações de influência exploram divisões em nossa sociedade usando vulnerabilidades do nosso ecossistema de informações. Eles tiram proveito de nosso compromisso com a liberdade de expressão e o livre fluxo de ideias. As plataformas de mídia social não podem, e não devem, ser as únicas defensoras da democracia e do discurso público (DIRESTA, 2018).

[35] Original: "'*If politics is an expression of our human will, on individual and collective levels, then the attention economy is directly undermining the assumptions that democracy rests on.' If Apple, Facebook, Google, Twitter, Instagram and Snapchat are gradually chipping away at our ability to control our own minds, could there come a point, I ask, at which democracy no longer functions*?" (LEWIS, 2017).

CAPÍTULO 4

Formas de Resistência ao Capitalismo de Vigilância: É possível combater as *big tech*?

No cenário atual, não temos escolha quanto à constante vigilância do nosso cotidiano. As tarefas mais comuns como, estudar, pedir comida, ou até mesmo praticar uma religião passaram a ser mediadas por aparelhos conectados à Internet; especialmente após a pandemia do novo coronavírus, quando foram impostas medidas de distanciamento social em diversos países e muitos tiveram que se render ao uso de novas tecnologias. Não é mais possível estar fora da Internet: certas contas só podem ser pagas por *internet banking*¸ videochamadas são essenciais para o trabalho e a escola, assim como para a vida social (conversar com amigos e família, por exemplo).

Como consequência, nesse processo, nossos dados são coletados por agentes públicos e privados que passam a deter quantidades sem precedentes de informações sobre nós. O *Big Data*, portanto, contribui para a produção de uma assimetria de informação que favorece os detentores dos dados e nos coloca – os usuários – em uma posição de desvantagem, como marionetes manipuladas por cordas invisíveis. Dessa maneira, aqueles têm poder sobre nosso movimento, crédito, emprego, educação; o que dificulta formas de exercer resistência, mas não as impossibilita (BRUNTON & NISSENBAUM, 2015, p. 49-55).

Este capítulo, então, tem como objetivo identificar algumas dessas técnicas, de modo a trazer um ar de esperança a esse fenômeno tão sufocante. Por meio da mobilização do princípio da privacidade, mostraremos como modificações no âmbito privado, assim como no aparato legal e movimentações da sociedade civil têm sido implementadas nos últimos anos para lutar contra as amarras do capitalismo de vigilância.

Como discutido no Capítulo 1, entre o final do século XX e ao longo do século XXI, o entendimento de privacidade evoluiu para o *status* de direito, de princípio fundamental (MULHOLLAND, 2018, p. 172; ABU-LABAN, 2012, p. 420). Nesse sentido, de acordo com Evgeny Morozov (2019), as interpretações

voltadas para a garantia da dignidade e liberdade do indivíduo desconsideram a questão econômica atrelada à privacidade: com a emergência das *big tech*, o "*big money*" e o "*big state*" tiveram sua relação com a tecnologia modificada, formando uma "*troika*" fortemente interligada. Portanto, serão necessárias modificações drásticas para combater essa concentração de poder, começando pela contestação desta (MOROZOV, 2019).

O atual modelo econômico nos paralisa. Por estar tão disperso no nosso cotidiano, é difícil perceber sua operação e constante manipulação (ZUBOFF, 2019, p. 492). Ademais, quando aliado ao Estado, "esse sistema pode se tornar uma ameaça existencial aos usuários". O Sistema de Crédito Social da China é talvez o exemplo mais drástico, mas bastante ilustrativo: ao monitorar os cidadãos 24 horas por dia por meio de aplicativos de celular e sensores dispersos pelo país, o governo consegue determinar quem está agindo ou não conforme as regras e padrões do partido, recompensando os primeiros e punindo os desviantes. Dentre as restrições, estão a impossibilidade de comprar passagens de ônibus ou trem, se candidatar a um emprego ou matricular o filho em determinadas escolas (DEIBERT, 2018, p. 417-8, tradução minha[1]).

Nesse sentido, Ronald Deibert, argumenta que é preciso pensar nas ameaças impostas pela tecnologia sobre nós enquanto uma questão de segurança, cuja solução passa pela expansão do controle de dados por parte dos indivíduos. O autor entende que é preciso ir além da ideia de "direito à privacidade", adotando uma abordagem humanizada quanto à cibersegurança que coloque os interesses individuais no centro da discussão e faça da privacidade um dos componentes da segurança (DEIBERT, 2018, p. 418).

Já para Shoshana Zuboff, a assimetria de poder presente atualmente coloca em risco a defesa da democracia enquanto o modelo político capaz de garantir liberdade individual. É preciso, assim, proteger as instituições democráticas, assegurando o debate e a troca de ideias necessárias para lutar contra as formas de injustiça presentes hoje (ZUBOFF, 2019, p. 519).

[1] Original: "*When companies share this data with governments, the system can become an existential threat to users*" (DEIBERT, 2018, p. 417-8).

Ademais, o argumento de que a vigilância é necessária para o exercício da segurança nacional ou de um mercado mais eficiente não pode mais ser aceito. O entendimento atual de privacidade, expresso por exemplo em relatórios não-governamentais, nacionais e internacionais, evidencia os problemas advindos da vigilância sistêmica e destaca o papel das instituições legais na viabilização desse fenômeno. Como consequência, estas passaram a perceber a necessidade de flexibilizar suas práticas e discursos quanto à vigilância: é preciso reavaliar os instrumentos regulatórios e exercer um monitoramento mais rígido das práticas de vigilância. Para isso, é necessária uma evolução drástica do sistema regulatório, que devido à sua lentidão e pouco conhecimento técnico, tem sido bastante ineficiente. Nesse sentido, a maior participação da sociedade civil nesses espaços pode ser uma fonte importante de debate e informação (REGAN, 2012, p. 403).

Em discussões em organizações internacionais como o Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE, em inglês) e o World Wide Web Consortium (W3C), então, "as proteções de privacidade foram vistas como um componente-chave no estabelecimento de sistemas confiáveis de informação em rede" e novos mecanismos de proteção dos usuários foram pensados. Entre esses, o Rathenau Institute of the Royal Netherlands Academy of Sciences e o Computer Science and Telecommunications Board of the US National Research Council estabeleceram fóruns de debate entre especialistas técnicos e políticos, que levaram à publicação de diversos relatórios sobre políticas e propostas técnicas. E o Projeto Platform for Privacy Preferences (P3P) de 1998 permitiu maior transparência na exposição das políticas de privacidades de serviços *online* (REGAN, 2012, p. 397-403, tradução minha[2]).

Fica evidente, no entanto, que não há um modelo único para a implementação de medidas de proteção da privacidade. Embora tenham objetivos semelhantes, as abordagens são únicas a cada país, seguindo as diretrizes de seus marcos legais, mas também padrões culturais, de forma que sejam aceitos socialmente (REGAN, 2012, p. 403). Isto é, como este capítulo pretende evidenciar, há um novo movimento global em torno da privacidade ainda muito ligado às elites, mas que visa a criação de uma "cultura de preocupação quanto à coleta,

[2] Original: "*Privacy protections were viewed as a key component in establishing trustworthy networked information systems"* (REGAN, 2012, p. 403).

compartilhamento e uso de informações pessoais - e com o conjunto de leis e políticas" recém-criado (RULE, 2012, p. 66, tradução minha[3]). Devido à ausência de uma definição única, o termo "privacidade" é facilmente compreendido, tendo um enorme apelo global e um significado para cada pessoa ou grupo (BENNETT, 2012, p. 418). Com isso, este é um termo capaz de transnacionalizar a luta contra o capitalismo de vigilância.

4.1 As *big tech* arrependidas

Conforme a tecnologia se torna mais sofisticada e as técnicas de *machine learning* evoluem, mais automáticos são os processos e as tomadas de decisão pelas máquinas. "A vocação que os algoritmos têm para penetrar em diversos âmbitos do nosso cotidiano já é vista como um fato da vida. Eles realizam tarefas que dificilmente pensaríamos em cumprir sem que houvesse um ser humano diante delas." Porém, nesse processo, parte do controle sobre esses algoritmos é perdida, pois eles são desenvolvidos para se automodificarem, o que confere opacidade à tecnologia (ALMEIDA & DONEDA, 2016).

Logo, aumenta a preocupação quanto às consequências dessa automação, que podem ir desde a reprodução de vieses e preconceitos, até possíveis distorções em decisões políticas, como processos eleitorais. Dessa forma, "é importante enfatizar a necessidade de verificar se [os algoritmos] estão sendo usados dentro da lei e da ética" (ALMEIDA & DONEDA, 2016; ZICARI, 2019).

Isto é, nas discussões atuais quanto ao controle das empresas de tecnologia, alguns dos principais caminhos defendidos são a regulação (assunto a ser aprofundado na próxima seção) e a ética, as medidas que podem ser implementadas pelas próprias empresas visando a redução de riscos perpetuados por seus produtos e serviços. Entre estas, podemos citar a "governança dos algoritmos", que "pode variar desde os pontos de vista estritamente jurídico e regulatório até uma postura puramente técnica", priorizando "a responsabilização, a transparência e as garantias técnicas" (ALMEIDA & DONEDA, 2016).

[3] Original: "*In fact, [national privacy codes] reflect a global culture of privacy protection lore, with principles embodied in earlier laws and policy statements heavily shaping those that have followed*" (RULE, 2012, p. 66).

Nesse sentido, a governança busca esclarecer os processos e implicações dos algoritmos através de mecanismos de monitoramento e prestação de contas, reduzindo a opacidade dessas tecnologias e definindo os responsáveis pelo seu uso, se o criador ou quem o emprega, além do estabelecimento de princípios éticos quanto ao uso de dados pessoais (ALMEIDA & DONEDA, 2016).

> As garantias técnicas são outro recurso fundamental, de maneira a estabelecer opções para o projeto de algoritmos quanto à mineração e análise de dados com considerações que busquem evitar preconceito, desigualdade ou quaisquer outros resultados tendenciosos. Nesse âmbito, os engenheiros e pesquisadores estão desenvolvendo técnicas para assegurar que os algoritmos e a sua implementação atendam aos padrões de concepção, desempenho e mesmo responsabilização. Num momento seguinte, existem técnicas de auditoria que podem ser úteis para determinar se o algoritmo adere às normas técnicas exigidas (ALMEIDA & DONEDA, 2016).

Como destaca Giovanni Buttarelli, Supervisor Europeu de Proteção de Dados da União Europeia entre 2009-2014, em entrevista a Roberto Zicari (2019), é preciso um esforço coletivo para garantir uma abordagem ética em torno da tecnologia: de desenvolvedores de tecnologia e prestadores de serviços, especialistas em ética e antropólogos, a reguladores e autoridades de supervisão, defensores dos direitos humanos e organizações da sociedade civil, "todos devem se envolver neste debate" (ZICARI, 2019, tradução minha[4]).

No âmbito do setor privado, segundo Danilo Doneda e Virgílio Almeida, a ética "deve ser parte da organização interna das empresas", presente em todas as etapas da produção, desde a maneira como os produtos são projetados até sua implementação e na relação com os usuários e clientes, mas também na forma como as empresas se relacionam com o interesse público, definindo "um processo de revisão e um órgão interno para garantir a integridade e conformidade com valores de interesse público quando usarem algoritmos" (ALMEIDA & DONEDA, 2016).

Dada a gravidade das consequências provocadas pelas tecnologias desenvolvidas por empresas como Google e Facebook – especialmente quanto ao exercício da democracia –, estas precisam ser responsabilizadas e trazer soluções aos problemas que criaram. "'*AI is now the most fashionable pretext for collecting*

[4] Original: "*From tech developers and service providers, to regulators and supervisory authorities, ethicists and anthropologists, civil society organisations and human rights defenders, and representatives of these from all regions of our planet, everyone must engage in this debate*" (ZICARI, 2019).

data. The long honeymoon with big tech is over. But they need to be part of the solution no longer part of the problem'"[5] (ZICARI, 2019).

Para Buttarelli, as empresas devem aprender que se não respeitarem os direitos e a dignidade de seus clientes, estes perderão a confiança nelas e as deixarão. Como consequência, elas enfrentarão danos à reputação e sanções. "E, terceiro, seu modelo de negócios não tem sucesso no longo prazo. Então, repito: a verdadeira inovação é inovação responsável" (ZICARI, 2019, tradução minha[6]).

Em suma, é preciso descentralizar a Internet, dando mais poder aos indivíduos sobre a forma como usam a tecnologia. Para isso, podem ser implementados, por exemplo, princípios de *accountability* e privacidade por padrão e por *design* (ZICARI, 2019), além de "*non addiction by design*" (DIAS, 2020), sempre mantendo a ética como fundamento norteador. Dentre estes, o princípio de privacidade por *design* se tornou um dos mais disseminados entre as medidas de proteção da privacidade por conta, principalmente, do Regulamento Geral sobre a Proteção de Dados (GDPR em inglês), que defende que "empresas devam desenvolver produtos e serviços com o pressuposto padrão de que eles protegem a privacidade, os dados e as informações dos titulares dos dados" (PENNEY et al, 2018, p. 106, tradução minha[7]).

Uma outra abordagem poderia ser o princípio de "direitos-humanos-por-*design*", o qual obriga o comprometimento dos desenvolvedores com o respeito e a garantia da privacidade enquanto um direito humano. Nesse sentido, há uma recusa por parte dos trabalhadores de viabilizar o desenvolvimento de ferramentas e armas de vigilância em massa e outras tecnologias que violam os direitos humanos e o direito internacional. Um exemplo foi a assinatura por parte de mais de quatro mil funcionários do Google de uma carta condenando a participação da empresa no Projeto Maven, uma iniciativa do exército estadunidense para integrar vigilância por *drones* e *machine learning*. Como consequência, o Google adotou uma série de

---

[5] Tradução: IA é agora o pretexto mais moderno para a coleta de dados. A longa lua de mel com as *big tech* acabou. Mas eles precisam fazer parte da solução e não mais fazer parte do problema (ZICARI, 2019).

[6] Original: "*And third, your business model is not successful in the long-term. So I repeat: real innovation is responsible innovation*" (ZICARI, 2019).

[7] Original: "*The overarching principle is that companies must design products and services with the default assumption that they protect privacy, data, and information of data subjects*" (PENNEY et al, 2018).

medidas para coordenar atividades de pesquisa e desenvolvimento em relação à inteligência artificial, e o contrato não foi renovado (PENNEY et al, 2018, p. 106-7).

Os *data scientists*, então, têm um papel especialmente importante no desenvolvimento de tecnologias mais éticas devido à sua capacidade técnica e à possibilidade de mudança "de dentro para fora." Isto é, enquanto integrantes das empresas do capitalismo de vigilância e, de certa forma, responsáveis pela criação desses mecanismos, eles poderiam advogar por medidas de redução de impacto provocado pelos algoritmos (D'ALESSANDRO et al., 2017). O que podemos ver claramente no documentário *O dilema das redes* (2020), onde vários funcionários de empresas como Google, Facebook, Instagram e Pinterest discursam sobre como não previram os malefícios de suas criações e agora tentam encontrar meios de reverter a situação. Outro caso seria a atualização e o cumprimento de códigos de conduta já existentes como o *Computer Society's Engineer's Code of Ethics* elaborado pelo Instituto de Engenheiros Eletricistas e Eletrônicos (IEEE), que estabelece padrões éticos de segurança cibernética (PENNEY et al, 2018, p. 106-7).

Ademais, quando a iniciativa parte de figuras com maior destaque no setor privado, mais importância é atribuída pelas demais empresas. Diversas pesquisas comprovam o caráter racista de muitas tecnologias de reconhecimento facial (PETERS, 2020) e, após os protestos desencadeados pelo assassinato de George Floyd nos Estados Unidos em junho de 2020, as críticas quanto a esses sistemas aumentaram exponencialmente. Em resposta, o atual CEO da IBM, Arvind Krishna, anunciou em uma carta ao Congresso norte-americano o fim da venda de produtos de análise e reconhecimento facial de uso geral por parte da empresa e elencou medidas de promoção de igualdade racial. Na carta, Krishna destaca o caráter igualitário da empresa, que desde a década de 1950 advoga pela igualdade de oportunidades, e pede ao Congresso medidas mais concretas quanto ao uso responsável da tecnologia, reforma policial e ampliação de oportunidades educacionais (IBM, 2020).

Para Tristan Harris (2020), nunca houve um momento tão propício para a mudança das *big tech*. Segundo o ex-funcionário do Google, a pandemia do novo

corona vírus evidenciou a importância dessas empresas quanto à informação do público geral e se mostrou um possível ponto de virada para esse modelo econômico predatório (HARRIS, 2020).

> *In the developing world, a hoax claimed India had banned coronavirus social posts, and in the US, 13 percent of people thought coronavirus was a hoax during the critical weeks where earlier notification to shelter-in-place would have saved thousands of lives. Tech platforms have an ability through their persuasive techniques and microtargeting to influence the behavior of society in ways traditional media can't. (...)*
> *The pandemic gives us a chance to convert online lawlessness into humane and regenerative technology* (HARRIS, 2020)[8].

Atualmente, essas empresas não podem mais fugir dos problemas que causaram. É preciso que elas tomem responsabilidade por seus atos e proponham mudanças reais. Harris argumenta que, em primeiro lugar, as plataformas de redes sociais devem abandonar a falsa ideia de que seus serviços são neutros e passar a de fato apoiar o interesse público: apoiando os profissionais de saúde nas linhas de frente, promovendo comunicação pública realmente eficaz e priorizando meios para uma ajuda mútua mais eficiente. Trata-se, portanto, de uma mudança no DNA dessas empresas, que renunciariam a vigilância em massa e passariam a defender o bem coletivo (HARRIS, 2020).

Uma dessas plataformas que estariam dispostas a colaborar com um modelo de negócios mais ético pode ser representada pelo Discord. O aplicativo se mostrou bastante útil nos protestos *Black Lives Matter* como uma forma de centralizar informações e agregar participantes em torno da causa. Contudo, em 2017, o mesmo aplicativo proporcionou o espaço necessário para supremacistas brancos coordenarem os protestos em Charlottesville que causaram a morte de uma mulher e deixaram 34 feridos (BROWN, 2020).

Desde então, usuários e grupos são expulsos do aplicativo usando rastreamento de metadados em vez de endereços IP e os moderadores de um grupo

[8] tradução: No mundo em desenvolvimento, uma farsa alegou que a Índia proibiu as postagens sociais sobre o coronavírus e, nos Estados Unidos, 13% das pessoas pensaram que o coronavírus era uma farsa durante as semanas críticas em que a notificação prévia para se abrigar em casa teria salvado milhares de vidas. As plataformas de tecnologia têm a capacidade de, por meio de suas técnicas persuasivas e microssegmentação, influenciar o comportamento da sociedade de uma forma que a mídia tradicional não consegue. (…) A pandemia nos dá a chance de converter a ilegalidade *online* em tecnologia humana e regenerativa (HARRIS, 2020).

podem adicionar *bots* para procurar por linguagem ofensiva e conseguem reportar mau comportamento mais rapidamente. Além disso, o Discord implementou um departamento de Confiança e Segurança (*Trust and Safety*), que representa 15% do quadro de funcionários da empresa e procura ativamente por grupos nacionalistas brancos e plataformas online que possam fazer uso de novos servidores no Discord (BROWN, 2020).

Como a atual pandemia levou ao fechamento de escolas e faculdades, mas também a migração do convívio social para o meio virtual, o aplicativo, que originalmente se mostrou bastante popular entre grupos de jogadores de videogames, atualmente tem diversos participantes dedicados a grupos de estudos, clubes de livros e até escoteiros (BROWN, 2020).

4.2 O fim da autorregulação?

Como regular os espaços virtuais é um assunto de grande debate desde a origem destes. Um dos poucos consensos, porém, é a ideia de que o direito internacional deve ser aplicado ao ambiente *online* da mesma forma que ocorre *offline*. Ademais, seguindo uma abordagem humanizada quanto à cibersegurança, os principais beneficiários dessa proteção legal são os indivíduos. Embora tenha sido desenvolvido para coordenar a relação entre os Estados, a evolução histórica do direito internacional trouxe os cidadãos para o centro de seu escopo de proteção (DEIBERT, 2018, p. 413). Hoje, então, torna-se essencial desenvolver e aplicar medidas regulatórias sobre as empresas de tecnologia para que garantam os direitos individuais *online*.

> *An essential part of a human-centric approach would therefore involve persistent critical interrogation, including reverse engineering, of both technologies and the institutions that promote and sustain them. This should not only be seen as a right of inquiry but also as an essential ingredient of a critical democratic society. Research that "lifts the lid off" the technology that surrounds us to reveal hidden security and privacy risks is essential to human rights, regardless of whether companies bristle at the exposure or threaten legal action* (DEIBERT, 2018, p. 421)[9].

[9] Tradução: Uma parte essencial de uma abordagem centrada no ser humano envolveria, portanto, interrogatório crítico persistente, incluindo engenharia reversa, tanto das tecnologias quanto das instituições que as promovem e sustentam. Isso não deve ser visto apenas como um direito de investigação, mas também como um ingrediente essencial de uma sociedade democrática crítica. A

É preciso, portanto, ter conhecimento de possíveis violações de direitos humanos na Internet e advogar pela proteção destes. Dessa maneira, mais atenção coletiva estará concentrada "na melhor forma de sustentar um ambiente de comunicação comum em que os direitos sejam protegidos em um espaço político cada vez mais comprimido." Pois, devido à imposição de regras, são definidos padrões de progresso e há um desincentivo a comportamentos desviantes, com os responsáveis levados a justificar suas ações para além de seu interesse próprio (DEIBERT, 2018, p. 422, tradução minha[10]).

No entanto, embora tenham havido importantes avanços na regulação do ciberespaço, os desafios do capitalismo de vigilância e do *big data* estão além das capacidades de muitos dos marcos legais atuais: "*[c]urrent privacy laws are not well adapted to the privacy concerns that arise in the big data context, in which risks tend to be probabilistic and data is aggregated*"[11] (STRANDBURG, 2014, p. 31). Com a violação constante da privacidade em favor da coleta e processamento predatórios de dados pessoais, são necessárias adaptações ou mesmo novas medidas regulatórias capazes de proteger os direitos individuais dos usuários.

Nesse sentido, um dos caminhos adotados foi o princípio de "*notice and consent*", por meio do qual, devido ao poder concentrado no setor privado, pouco foi feito com relação à regulação das empresas de tecnologia. Esperava-se que dessa forma a autorregulação em torno da garantia da privacidade fosse incentivada enquanto uma prática compartilhada no setor privado.

> *The notice and consent paradigm assumes that citizens are able to assess the potential benefits and costs of data acquisition sufficiently accurately to make informed choices. This assumption was something of a legal fiction when applied to data collected by government agencies and regulated industries in the 1970s. It is most certainly a legal fantasy today, for a variety of reasons including the increasing use of complex and opaque predictive data-mining techniques, the interrelatedness of*

pesquisa que "levanta a tampa" da tecnologia que nos rodeia para revelar riscos ocultos de segurança e privacidade é essencial para os direitos humanos, independentemente de as empresas se irritarem com a exposição ou ameaçarem uma ação legal (DEIBERT, 2018, p. 421).

[10] Original: "*it will help focus collective attention on how best to sustain a common communications environment in which rights are protected in an increasingly compressed political space*" (DEIBERT, 2018, p. 422).

[11] Tradução: As leis de privacidade atuais não estão bem adaptadas às questões de privacidade que surgem no contexto do *big data*, no qual os riscos tendem a ser probabilísticos e os dados agregados (STRANDBURG, 2014, p. 31).

> *personal data, and the unpredictability of potential harms from its nearly ubiquitous collection* (STRANDBURG, 2014, p. 8)[12].

Isto é, contar que as empresas fossem estabelecer um padrão de comportamento em prol da privacidade e que os usuários seriam capazes de ler e interpretar todas as políticas de privacidade dos produtos e serviços que viessem a usar se mostrou incompatível com a realidade por uma série de motivos. Um deles sendo a rapidez com que a tecnologia avança e a consolidação do capitalismo de vigilância, que prosperou em um ambiente tão pouco regulado (STRANDBURG, 2014).

Ademais, apesar do princípio de "*consent*" (consentimento) oferecer mais transparência ao indivíduo sobre a maneira como seus dados são usados, este se mostra ineficiente na prática, especialmente devido à falsa possibilidade de *opt-out*. Ou seja, o princípio-base de medidas como o *Personal Information Protection and Electronic Documents Act* **(**PIPEDA) do Canadá reforça a ideia de que se não concordarmos com algo quanto ao uso ou reprodução de nossos dados, podemos "escolher" não participar (KAK & RICHARDSON, 2020).

Consequentemente, caso a privacidade não seja garantida, tecnologias como a Internet das Coisas podem, ao invés de trazer praticidade à vida das pessoas, levar a mais pontos de vigilância, reforçando a assemblagem de vigilância. Ao aliar a informação coletada por sensores aos dados pessoais já conhecidos, uma série de correlações são confirmadas, levando a formas mais concretas de controle. "*In short, IoT allows for deeper scrutiny of individuals than ever before*"[13] (ALMEIDA et al, 2015, p. 57).

Assim, dada a variedade de questões advindas da tecnologia, as medidas legais em torno da proteção da privacidade devem ser modificadas conforme a natureza dos problemas que buscam tratar (ALMEIDA et al., 2015, p. 57). O que

[12] Tradução: O paradigma de notificação e consentimento pressupõe que os cidadãos são capazes de avaliar os benefícios e custos potenciais da aquisição de dados com suficiente precisão para fazer escolhas informadas. Essa suposição era uma espécie de ficção jurídica quando aplicada a dados coletados por agências governamentais e indústrias regulamentadas na década de 1970. É certamente uma fantasia legal hoje, por uma variedade de razões, incluindo o uso crescente de técnicas de mineração de dados preditivas complexas e opacas, a inter-relação de dados pessoais e a imprevisibilidade de danos potenciais de sua coleção quase onipresente (STRANDBURG, 2014, p. 8).

[13] Tradução: Em suma, a *IoT* [Internet das Coisas] permite um exame mais profundo dos indivíduos do que nunca (ALMEIDA et al, 2015, p. 57).

pode parecer lógico, mas nem sempre é o caso: muitas iniciativas buscam soluções universais que acabam não tendo os melhores resultados pois não tratam de fato a raiz da questão.

Isto posto, dentre as tendências mais comuns adotadas pelas medidas regulatórias, podemos destacar: a **minimização de dados**, que, indo na contramão da Internet das Coisas, onde o máximo de informação é coletada, indica que somente o mínimo necessário para executar determinado serviço deve ser coletado, garantindo maior eficiência ao processo. Além disso, os princípios de ***accountability*** (prestação de contas), "***notice and choice*"** (semelhante à autodeterminação informativa) e **acesso a dados pessoais** estabelecem, em linhas gerais, o direito de o usuário ter acesso e conhecimento sobre todos os dados sobre si conhecidos pelas empresas, além de poder escolher como estes são manipulados, o que exigiria um alto grau informacional do usuário, mas também uma infraestrutura sofisticada de interação entre ele e as empresas, assim como altos níveis de transparência no processo de coleta de dados e definições claras quanto aos responsáveis pelo tratamento destes (ALMEIDA et al., 2015, p. 57-8).

No plano internacional, então, muitas leis de proteção de dados, como a GDPR, articulam a garantia da privacidade por meio de mecanismos de maior *accountability* e transparência - alguns dos elementos destacados acima -, além de técnicas de "*data protection impact assessments*" (DPIAs), viabilizando uma proteção mais ampla. Pois, ao monitorar possíveis riscos advindos de sistemas de inteligência artificial, é possível também endereçar questões ligadas a *bias* e discriminação, indo além de temas ligados somente à privacidade (KAK & RICHARDSON, 2020).

Ademais, Amba Kak e Rashida Richardson (2020) alertam para o caráter coletivo presente em perspectivas voltadas para *accountability*. O *Canadian Treasury Board's 2019 Directive on Automated Decision Making* e o *Algorithmic Accountability Act of 2019*, um projeto de lei proposto nos Estados Unidos, por exemplo, exigem respectivamente que agências do governo federal e empresas avaliem possíveis impactos quanto à segurança e privacidade dos dados dos usuários, além de questões ligadas à parcialidade e discriminação, indo além de uma visão individualista da proteção de dados (KAK & RICHARDSON, 2020).

Porém, o foco em *accountability* pode ainda proporcionar maior transparência e participação civil, levando em consideração também questões políticas e econômicas:

> *As recent high-profile smart city projects indicate, large-scale AI projects lead to an increasing consolidation of power in the hands of private companies to make decisions about civic life. The #BlockSidewalk campaign notes that Toronto's Sidewalk Labs smart city project "is as much about privatization and corporate control as it is about privacy." Policies around AI must, therefore, be responsive to this broader political economy, and focus on ensuring that those directly impacted have a meaningful say in whether these systems are used at all, and in whose interest* (KAK & RICHARDSON, 2020)[14].

Além disso, outro princípio característico das leis de proteção de dados, a minimização de dados, preza pela coleta mínima na utilização de um serviço ou produto. A citar, recentemente o Regulador sueco de Proteção de Dados baniu sistemas de reconhecimento facial em escolas, a fim de evitar que essas informações sejam usadas para fins imprevistos. Segundo a decisão, o uso de dados faciais não é apropriado ou necessário para registrar a presença dos estudantes (KAK & RICHARDSON, 2020).

Contudo, é importante destacarmos uma questão preocupante quanto à formulação de medidas regulatórias: o nível de conhecimento sobre o assunto entre os órgãos legislativos. Como os depoimentos no Congresso norte-americano de Mark Zuckerberg logo após o escândalo da Cambridge Analytica (WATSON, 2018) mostram, os formuladores de decisão, as pessoas supostamente mais capacitadas do governo, não sabiam o que perguntar, seus questionamentos foram extremamente rasos. No entanto, é preciso ressaltar o papel dos defensores e ativistas da privacidade, cuja pressão pode influenciar significativamente a maneira que os reguladores operam. "*Without organized constituent pressure, lawmakers*

[14] Tradução: Como indicam projetos recentes de cidades inteligentes de alto nível, projetos de IA em grande escala levam a uma consolidação cada vez maior do poder nas mãos de empresas privadas para tomar decisões sobre a vida cívica. A campanha *#BlockSidewalk* observa que o projeto de cidade inteligente Sidewalk Labs de Toronto "trata tanto de privatização e controle corporativo quanto de privacidade". As políticas em torno da IA devem, portanto, responder a essa economia política mais ampla e focar em garantir que as pessoas diretamente afetadas tenham uma fala significativa sobre se esses sistemas sequer são usados e no interesse de quem (KAK & RICHARDSON, 2020).

are far more likely do nothing or create legislation favoring the very corporations that need regulating in the first place"[15] (GLASER, 2018).

> *In Facebook's case, this isn't hypothetical: Lawmakers are not hearing from the groups that focus on internet privacy and appear to be at a bit of a loss on how to proceed with legislation. "The conspicuous silence of the tech-oriented civil-society groups has been really telling," one congressional staffer told me, adding that "a grass-roots campaign to capitalize on the immense public interest in these issues" could help catalyze a push for comprehensive data-protection legislation in the vein of the General Data Protection Rule, or GDPR, the wide-ranging European Union regulation going into effect May 25 that will significantly change the ways companies like Facebook, Google, and Twitter operate in those countries* (GLASER, 2018)[16].

Isto é, o principal ponto a levar em consideração na formulação de políticas quanto à privacidade são as pessoas. Para desenvolver um sistema centrado nos direitos humanos, é necessário ter os usuários, os cidadãos, enquanto prioridade, pois estes são os beneficiários de qualquer medida e as vítimas de possíveis violações *(*ALMEIDA et al., 2015, p. 58). Porém, o papel desse grupo também é central para advogar por mudanças: "as organizações de defesa e ativistas profissionais desempenham um papel crítico e, quando trabalham juntos para estimular o público, podem dar ao espectro da regulamentação uma forma corporal" (GLASER, 2018).

4.3 Movimentos da Sociedade Civil

Muitos atores estão presentes nas disputas pelo controle da Internet, sendo o setor privado e o Estado dois dos com maior poder. No entanto, este também é um espaço para contestação individual. E à medida que a tecnologia avança num ritmo muito acelerado, há um descompasso em relação às políticas públicas e os

[15] Tradução: Sem a pressão organizada dos constituintes, é muito mais provável que os legisladores não façam nada ou criem legislações que favoreçam as próprias empresas que precisam de regulamentação em primeiro lugar (GLASER, 2018).

[16] Tradução: No caso do Facebook, isso não é hipotético: os legisladores não estão ouvindo os grupos que se concentram na privacidade na internet e parecem estar um pouco perdidos sobre como proceder com a legislação. "O silêncio notável dos grupos da sociedade civil voltados para a tecnologia tem sido realmente revelador", disse-me um membro do Congresso, acrescentando que "uma campanha de base para capitalizar o imenso interesse público nessas questões" poderia ajudar a catalisar um impulso para legislação abrangente de proteção de dados na linha da Regra Geral de Proteção de Dados, ou GDPR, a ampla regulamentação da União Europeia que entrará em vigor em 25 de maio que mudará significativamente a forma como empresas como Facebook, Google e Twitter operam nesses países (GLASER, 2018).

marcos regulatórios, que apesar de sua importância para o controle sobre a operação das empresas (BRUNTON & NISSENBAUM, 2015, p. 61), são marcados por processos muito demorados e burocráticos: "*While private corporations have more institutional flexibility (...), governments face greater rigidity, making it slower for them to adapt and respond to these changes*"[17] (HUREL, 2016, p. 38-9). Portanto, o papel da sociedade civil e dos indivíduos é particularmente importante na contestação do controle da Internet e na luta pela defesa da privacidade, uma vez que representam os principais afetados por mudanças impostas por outros atores e devido a sua capacidade de agência.

> *The Internet is not a mechanism, it is gradually becoming part of our social, economic and political relations, and tackling the governance challenges that emerge with it is also understanding what political, social and economic changes awaits. What kind of governance and security do we wish to see in this interconnected future?* (HUREL, 2016, p. 72-3)[18].

Conforme a tecnologia se torna cada vez mais intrínseca ao nosso cotidiano e mais precisas são as recomendações de serviços como Google e Amazon, a conveniência pode se confundir com manipulação (LANIER & EUCHNER, 2019, p. 15). Abrir seu *e-mail* e descobrir uma oferta para aquela televisão nova que você tanto quer comprar ou começar a digitar "televisão" no Google e entre os resultados aparecerem diversos anúncios com o modelo e a marca desejados pode parecer muito prático, mas como esses serviços foram capazes de determinar que essa seria sua próxima pesquisa? É aterrorizante pensar o quanto somos vigiados o tempo todo, o que sabem sobre nós sem o nosso consentimento.

O capitalismo de vigilância nos vende a falsa ideia de que somos nós quem determinamos o que queremos procurar *online*. No entanto, o que o Google faz, por exemplo, é tentar manipular nossas pesquisas de forma a atrair mais dinheiro para si, satisfazendo os desejos de seus clientes. Portanto, se conseguirmos retomar ao menos parte de nossa agência *online*, teremos muito mais controle sobre o *offline*,

[17] Tradução: Enquanto as empresas privadas têm mais flexibilidade institucional (...), os governos enfrentam maior rigidez, tornando mais lento para eles se adaptarem e responderem a essas mudanças (HUREL, 2016, p. 38-9).

[18] Tradução: A Internet não é um mecanismo, ela está gradualmente se tornando parte de nossas relações sociais, econômicas e políticas, e enfrentar os desafios de governança que surgem com ela também é entender o que as mudanças políticas, sociais e econômicas são esperadas. Que tipo de governança e segurança desejamos ver neste futuro interconectado? (HUREL, 2016, p. 72-3).

sobre nossas decisões políticas e econômicas (LANIER & EUCHNER, 2019, p. 16).

> *A world in which you have more agency and you're more in control might be a little more work for you, but it would be much, much easier to tell that you were actually driving and not being manipulated. It probably wouldn't even be more work for you. In fact, one of the things that is really interesting is that when you take people who are used to receiving news feeds that are formulated by an algorithm and they switch instead to self-directed news gathering through search and so forth, not only do they become better informed by every measure, but they do so with vastly less time. And this is an experiment that's been repeated multiple times* (LANIER & EUCHNER, 2019, p. 16)[19].

Trata-se, então, de resistir ao modelo econômico atual, de encontrar maneiras de contestar o poder concentrado nas mãos do setor privado. E embora alguns defendam a ideia de se desligar das redes sociais e outros mecanismos de vigilância (DILEMA DAS REDES, 2020), isso implicaria na perda das vantagens advindas da tecnologia: é um *trade off* injusto em que se deve escolher entre a participação às custas de nossos dados, de nossa privacidade, e não participar, mas "ser um *nobody*", estar desconectado dos outros (RAYNES-GOLDIE, 2007).

Além disso, tal sugestão está em descompasso com o contexto atual. "Parece simples para um ex-executivo das big techs proibir o filho de ter qualquer contato com tecnologia (...). Mas como falar isso para as crianças cada vez mais dependentes da tecnologia até mesmo para estudar num mundo que atravessa uma pandemia?" (DIAS, 2020).

Isto posto, também é preciso levar em consideração o que muitas pessoas entendem como a Internet. Em países como Brasil e Myanmar – como mostra o documentário *O dilema das red*es (2020) –, a maioria dos pacotes de dados vendidos pelas empresas de telecomunicação oferecem acesso gratuito ao Facebook, Instagram e Whatsapp. "Criou-se um mercado do qual é praticamente impossível sair: as pessoas confundem internet com as interações que acontecem

[19] Tradução: Um mundo no qual você tem mais agência e está mais no controle pode dar um pouco mais de trabalho para você, mas seria muito, muito mais fácil dizer que você estava realmente dirigindo e não sendo manipulado. Provavelmente nem seria mais trabalho para você. Na verdade, uma das coisas que é realmente interessante é que quando você pega pessoas que estão acostumadas a receber *feeds* de notícias formulados por um algoritmo e, em vez disso, mudam para a coleta autodirigida de notícias por meio de pesquisa e assim por diante, não apenas tornam-se mais bem informados por todas as medições, mas o fazem em muito menos tempo. E este é um experimento que foi repetido várias vezes (LANIER & EUCHNER, 2019, p. 16).

nessas plataformas, e toda a vida acontece ali." Assim, muitos entendem que tudo que se pode fazer no celular é usar aplicativos já instalados no aparelho sem pagar nada por isso. Como, então, pedir a eles que abandonem esses serviços? (DIAS, 2020).

Apesar disso, a resistência pode ser exercida de diversas maneiras. Geralmente motivado por questões políticas, esse movimento age como um desafio ao *status quo*, criando atrito nos sistemas existentes de dominação e controle, atuando de maneira oculta e informal em grande parte dos casos. "*Instead of being in opposition to power, resistance is necessary and co-productive of the forms that power takes, including the control mechanisms through which power manifests and becomes visible (e.g. architecture, law, norms)*"[20] (GILLIOM & MONAHAN, 2012, p. 405-7).

Resistir é uma prática cultural capaz de produzir identidades, é um exercício de agência, de contestação para além da reprodução das relações de poder. Em última instância, trata-se de uma prática "generativa e autoafirmativa." "*Through resistance, people test boundaries, build sociality, and achieve dignity, both within and between institutional structures and dominant cultural logics*"[21] (GILLIOM & MONAHAN, 2012, p. 407). Ademais,

> *The secrets of everyday resistance are fundamentally contrary to the principles of surveillance in ways that more public and typical forms of opposition to surveillance cannot be. There is, therefore, a sense in which practices of everyday resistance against surveillance do more than merely trick the monitoring program in question. Because these acts of resistance are typically hidden, they also offer a broader ideological challenge to the forced visibility that is central to surveillance societies. Widespread patterns of everyday resistance carry with them a necessary challenge to the very organizing principles of the surveillance society and are, therefore, far more important than a simple, straight-on assessment of their political and social importance might suggest* (GILLIOM & MONAHAN, 2012, p. 410)[22].

[20] Tradução: Em vez de estar em oposição ao poder, a resistência é necessária e co-produtiva das formas que o poder assume, incluindo os mecanismos de controle através dos quais o poder se manifesta e se torna visível (por exemplo, arquitetura, lei, normas) (GILLIOM & MONAHAN, 2012, p. 406-7).

[21] Tradução: Por meio da resistência, as pessoas testam limites, constroem sociabilidade e alcançam dignidade, tanto dentro como entre as estruturas institucionais e lógicas culturais dominantes (GILLION & MOHAHAN, 2012, p. 407).

[22] Tradução: Os segredos da resistência cotidiana são fundamentalmente contrários aos princípios da vigilância de maneiras que as formas mais públicas e típicas de oposição à vigilância não podem ser. Há, portanto, um sentido em que as práticas de resistência cotidiana contra a vigilância fazem mais do que simplesmente enganar o programa de monitoramento em questão. Como esses atos de

Portanto, as possibilidades de exercer resistência contra o capitalismo de vigilância são diversas, mas em sua maioria caracterizadas pelo caráter da invisibilidade, próximas à ideia de camuflagem. Assim como soldados em campo formam um padrão, tornando-os invisíveis em meio a tantos outros vestindo uniformes que se misturam ao ambiente, a camuflagem *online* diz respeito à capacidade de passar despercebido pelos mecanismos de vigilância sem perder os benefícios advindos da participação; o que pode acontecer de diversas formas (BRUNTON & NISSENBAUM, 2015, p. 48).

Obfuscation, por exemplo, trata-se de uma técnica geralmente empregada por indivíduos ou grupos com pouco ou nenhum poder sobre os controladores de serviços digitais em que são produzidas informações confusas ou ambíguas para deliberadamente interferir sobre a coleta de dados e a vigilância. É uma forma de produzir ruído suficiente para tornar os dados coletados inutilizáveis, de se camuflar em uma imensidade de informações (BRUNTON & NISSENBAUM, 2015).

> *Obfuscation, at its most abstract, is the production of noise modeled on an existing signal in order to make a collection of data more ambiguous, confusing, harder to exploit, more difficult to act on, and therefore less valuable. The word "obfuscation" was chosen for this activity because it connotes obscurity, unintelligibility, and bewilderment and because it helps to distinguish this approach from methods that rely on disappearance or erasure. Obfuscation assumes that the signal can be spotted in some way and adds a plethora of related, similar, and pertinent signals—a crowd which an individual can mix, mingle, and, if only for a short time, hide* (BRUNTON & NISSENBAUM, 2015, p. 46)[23].

A depender do adversário, do ator de quem se tenta proteger, e das situações em que a *obfuscation* é empregada, os meios utilizados variam (BRUNTON & NISSENBAUM, 2015, p. 84). No caso do Google, o *software TrackMeNot* foi desenvolvido em 2006 em resposta ao pedido do Departamento de Justiça dos

---

resistência são tipicamente ocultos, eles também oferecem um desafio ideológico mais amplo à visibilidade forçada que é central para sociedades de vigilância. Padrões generalizados de resistência cotidiana trazem consigo um desafio necessário aos próprios princípios organizadores da sociedade de vigilância e são, portanto, muito mais importantes do que uma avaliação simples e direta de sua importância política e social pode sugerir (GILLIOM & MONAHAN, 2012, p. 410).

[23] Tradução: A ofuscação, em sua forma mais abstrata, é a produção de ruído modelado em um sinal existente para tornar uma coleção de dados mais ambígua, confusa, mais difícil de explorar, mais difícil de agir e, portanto, menos valiosa. A palavra "ofuscação" foi escolhida para esta atividade porque conota obscuridade, ininteligibilidade e perplexidade e porque ajuda a distinguir essa abordagem de métodos que dependem do desaparecimento ou apagamento. A ofuscação assume que o sinal pode ser detectado de alguma forma e adiciona uma infinidade de sinais relacionados, semelhantes e pertinentes - uma multidão em que um indivíduo pode se misturar, circular e, mesmo que apenas por um curto período de tempo, esconder (BRUNTON & NISSENBAUM, 2015, p. 46).

Estados Unidos pelos históricos de pesquisa mantidos pela empresa. Ao fazer uma busca, automaticamente são geradas diversas outras que tentam imitar o comportamento de pesquisa de usuários reais. Dessa maneira, o mecanismo esconde as reais consultas dos usuários em meio a várias outras produzidas artificialmente, dificultando a produção de um perfil preciso (BRUNTON & NISSENBAUM, 2015, p. 13-4).

Já o *FaceCloak*, busca limitar o acesso do Facebook a informações pessoais dos usuários. Ao usar o serviço, é possível escolher se informações como lugar onde estudou ou cidade onde mora são exibidas abertamente ou mantidas privadas, o que determina se serão transmitidas aos servidores da rede social. Ao escolher mantê-las privadas, o Facebook nunca tem acesso às informações, pois são fabricadas outras quaisquer, sem relação com a realidade do usuário. As reais são enviadas para um servidor separado onde são criptografadas e poderão ser de-criptografadas e exibidas somente para amigos autorizados que acessem sua página usando o *plug-in* do *FaceCloak* (BRUNTON & NISSENBAUM, 2015, p. 39-40).

Por outro lado, denunciar os abusos exercidos pelas *big tech* também pode ser uma forma de resistir, de contestar as assimetrias de poder. O movimento *Sleeping Giants*, por exemplo, começou como um esforço do publicitário Matt Rivitz de alertar grandes marcas sobre os perigos da publicidade programática, sobre anúncios em *sites* da extrema direta e de compartilhamento de *fake news*. Criada em 2016, a conta no Twitter é descrita como: "'Um movimento para tornar o fanatismo e o sexismo menos lucrativos'" (QUEIMALIÑOS, 2020).

Já presente em onze países, o movimento segue uma organização de células anônimas e independentes e enfraqueceu seriamente a estrutura de monetização de figuras ligadas à extrema direita. O *site Breitbart News*, cujo ex-diretor é Steve Bannon, ex-estrategista de Donald Trump, perdeu mais de €8 milhões em publicidade. Ademais, graças às denúncias do *Sleeping Giants*, o "investidor de ultradireita Robert Mercer se viu obrigado a deixar seu cargo de CEO na Renaissance Tecnhologies depois que vários clientes ameaçaram abandonar a empresa ao saber de sua relação com supremacistas brancos" e o "apresentador conservador Bill O'Reilly, da Fox, perdeu praticamente todos os seus anunciantes" (QUEIMALIÑOS, 2020).

Crítico do Google e Facebook, Rivitz chama atenção para a capacidade que essas duas empresas têm de perpetuar esse tipo de publicidade. O ativista advoga por mais transparência e prestação de contas e impulsionou a aprovação da "Emenda Sleeping Giants", uma regulamentação governamental francesa que visa "evitar que anunciantes financiem o ódio e o extremismo online", uma conquista importante na luta contra esse "sistema podre" (QUEIMALIÑOS, 2020).

Ademais, seguindo uma outra abordagem, estão aqueles que defendem uma nova economia da informação. Jaron Lanier, por exemplo, propõe a criação de um sistema de micropagamentos em troca dos dados fornecidos pelos usuários às empresas de tecnologia. Segundo o autor, se nossos dados são capazes de gerar tanto lucro para essas empresas, nós, enquanto fornecedores de matéria-prima, deveríamos ser pagos ao disponibilizar esse material; o que definitivamente não caracteriza o cenário atual. "*What the AI companies are really saying is that once we have your information, it's suddenly valuable, but that when you had it, it was worthless. We have the right to treat it as valuable and you don't*"[24] (LANIER & EUCHNER, 2019, p. 16).

Por meio desse sistema, os usuários seriam incentivados a gerar dados em maior quantidade e qualidade, pois isto resultaria em melhores lucros. Ademais, de acordo com Lanier, esse seria o caminho para uma sociedade mais automatizada e eficiente, com os dados usados para garantir bens comuns ao invés de perpetuar um sistema predatório (LANIER & EUCHNER, 2019, p. 16).

> *The philosophy we're working with is that the productivity improvements and well-being improvements brought about by the Internet are hidden economically because everything is free. Once they're revealed, they will turn up the economy. A big company would get a smaller slice of a larger pie, but we should start to see a growing economy based on monetizing information. That has to be the right long-term strategy for some sort of highly automated and efficient world of the future with higher levels of technology. I just don't see any other alternatives* (LANIER & EUCHNER, 2019, p. 17)[25].

[24] Tradução: O que as empresas de IA realmente estão dizendo é que, uma vez que temos suas informações, de repente elas são valiosas, mas quando você as tem, elas não têm valor. Temos o direito de tratá-lo como algo valioso e você não (LANIER & EUCHNER, 2019, p. 16).

[25] Tradução: A filosofia com a qual estamos trabalhando é que as melhorias de produtividade e bem-estar trazidas pela Internet são economicamente ocultas porque tudo é gratuito. Assim que forem revelados, eles irão aumentar a economia. Uma grande empresa ficaria com uma fatia menor de um bolo maior, mas devemos começar a ver uma economia crescente baseada na monetização de informações. Essa deve ser a estratégia certa de longo prazo para algum tipo de mundo do futuro

Portanto, ao transformar nossos dados em um ativo, teríamos mais controle sobre quem os acessa e possivelmente mais poder de barganha com as *big tech* (MOROZOV, 2013). No entanto, segundo Evgeny Morozov, apesar da importância do aspecto econômico, também é preciso considerar uma mudança mais estrutural, a nível institucional. Para realmente alterar a atual assimetria de poder que beneficia o setor privado, serão necessárias drásticas modificações estruturais (MOROZOV, 2020).

> *The great social democratic achievements of the twentieth century were in institutional innovation. By engaging with the risks posed to democracy by Big Tech, social democracy can both revive this tradition and reimagine its role. But that means leaving the comfort zone of regulation and campaigning for radically different technological infrastructures* (MOROZOV, 2020)[26].

É preciso ir além das soluções convencionais e imaginar configurações alternativas de poder. Especialmente após o novo corona vírus, devemos reinterpretar o novo ecossistema digital e elaborar um novo conjunto de instituições para tornar nossa sociedade mais eficaz e eficiente e promover justiça, solidariedade e igualitarismo (MOROZOV, 2020).

"*The challenge at present is to preserve at least the possibility of reconquering that infrastructure*."[27] Para além da regulação, é preciso pensar em novas agendas políticas e econômicas que levam o papel das *big tech* em consideração, assim como a garantia da privacidade. Trata-se da redefinição do modelo econômico (MOROZOV, 2020).

Em primeiro lugar, devemos definir as condições necessárias para esse projeto se concretizar, o que dependerá de financiamento, mas também de políticos e empresários dispostos a ir contra o *status quo*, a adotar uma postura anti-hierárquica. Passada essa fase de idealização, será preciso repensar a social

---

altamente automatizado e eficiente, com níveis mais elevados de tecnologia. Eu simplesmente não vejo nenhuma outra alternativa (LANIER & EUCHNER, 2019, p. 17).

[26] Tradução: As grandes conquistas da social-democracia do século XX foram na inovação institucional. Ao se envolver com os riscos apresentados à democracia pela *Big Tech*, a social-democracia pode reviver essa tradição e reimaginar seu papel. Mas isso significa sair da zona de conforto da regulação e fazer campanha por infraestruturas tecnológicas radicalmente diferentes (MOROZOV, 2020).

[27] Tradução: O desafio atual é preservar ao menos a possibilidade de reconquistar essa infraestrutura (MOROZOV, 2020).

democracia do século XXI e colocá-la em prática: como poderemos realinhar os direitos individuais e a lógica econômica (MOROZOV, 2020).

"*If we manage to achieve some progress on both of those fronts, there is a good chance that social democracy will not just survive but prosper*."[28] Pois, mesmo com os lucros e a constante expansão de empresas como Google e Facebook, sabe-se que suas operações são altamente custosas (MOROZOV, 2020). Custosas em termos econômicos, políticos e sociais. Diversos são os trabalhos, documentários e movimentos sociais que evidenciam esses custos: a privacidade, a liberdade e a democracia estão em risco. É preciso um movimento organizado em torno da reconfiguração desse sistema.

[28] Tradução: Se conseguirmos alcançar algum progresso em ambos as frentes, há uma boa chance da social-democracia não só sobreviver mas prosperar (MOROZOV, 2020).

Conclusão

Este trabalho tenta engajar com e contribuir para uma crescente literatura sobre o que Shoshana Zuboff nomeia "capitalismo de vigilância" (ZUBOFF, 2018; 2019). Ao mobilizar o princípio da privacidade como um direito fundamental, buscamos chamar atenção para as consequências sociais e políticas desse modelo econômico baseado na coleta e análise de dados pessoais.

O atual momento histórico é especialmente representativo dessas consequências e pode impulsionar ou retardar a expansão do capitalismo de vigilância. Com a pandemia, espaços e atividades antes pouco digitalizadas hoje só podem ser realizadas *online*. Ainda que antes os regimes de *home office* e *home school* fossem comuns para algumas pessoas, esta não era a regra. Nunca antes foram feitas tantas chamadas de vídeo: são escolas e faculdades, empresas, institutos de pesquisa, organizações internacionais e não governamentais e até órgãos do governo se readaptando a essa nova realidade.

Talvez este seja o momento de maior vigilância já visto. Conforme a Internet se popularizou, esta passou a ser a principal forma como buscamos informações, como nos conectamos com outras pessoas – é um espaço político e social por meio do qual expressamos nossas opiniões, realizamos trocas, consumimos entretenimento e muito mais (NISSENBAUM, 2010, p. 197-8). Porém, este também é um espaço de disputas. Desde que o Google inaugurou seu modelo de negócios baseado em propagandas direcionadas, a corrida pela elaboração de perfis mais precisos significou uma maior coleta de dados pessoais, o que, consequentemente, tornou a violação da privacidade uma prática disseminada entre as principais empresas baseadas em tecnologia e levou a um ambiente de constante vigilância (ZUBOFF, 2019). Nesse sentido, procuramos evidenciar ainda que o capitalismo da vigilância tem como fundamento a manipulação do comportamento humano e a dissolução da subjetividade em padrões de conduta, cujo objetivo é prever, antecipar e ditar nossas escolhas.

Ademais, o capitalismo de vigilância provocou uma acentuada assimetria de poder em favor das *big techs*. Sua lógica de acumulação e o ambiente de desregulação característico de seu momento de origem contribuíram para que esse modelo econômico se espalhasse pelo mundo e controlasse os fluxos de informações; em especial, informações sobre o comportamento humano. Logo, o conhecimento é concentrado nas mãos de poucas empresas, conferindo-lhes poder sobre o que e como conhecemos. "*As things currently stand, it is the surveillance capitalist corporations that know. It is the market form that decides. It is the competitive struggle among surveillance capitalists that decides who decides.*"[1] Assim, este é um momento de acentuação das desigualdades. Enquanto alguns sabem muito, nós estamos às cegas no que diz respeito ao que é conhecido sobre nós e o que é feito com essas informações (ZUBOFF, 2019, p. 186).

Tal cenário é ainda mais evidente especialmente em países como o Brasil, onde cerca de 30% da população não têm acesso à Internet e muitos dos que têm só conseguem acessar pelo celular (TENENTE, 2020), geralmente com pacotes de dados que oferecem acesso gratuito às redes sociais. Assim, com a pandemia, muitos estão literalmente desconectados – sem poder estudar, trabalhar ou mesmo conversar com amigos e familiares.

No primeiro capítulo, discutimos como a privacidade evoluiu ao longo do tempo e hoje é vista por muitos como um direito fundamental. E nos capítulos seguintes, mostramos como esse direito tem sido violado principalmente por empresas de tecnologia como Google e Facebook que prosperaram ao longo dos anos 2000 devido aos baixos níveis de regulação quanto ao ambiente virtual e à popularização de seus serviços. Contudo, como apresentado no quarto capítulo, os problemas econômicos, sociais e políticos dessa prática são cada vez mais conhecidos pela sociedade, que vem demandando mais formas de controle sobre essas empresas e sobre como manipulam nossos dados.

Ao passo que alguns advogam por maiores níveis de controle sobre o uso de nossos dados (ALMEIDA et al, 2015, p. 57-8), teóricos como Helen Nissenbaum

[1] Tradução: Como as coisas estão atualmente, é a vigilância das corporações capitalistas que sabe. É a forma de mercado que decide. É a luta competitiva entre os capitalistas de vigilância que decide quem decide (ZUBOFF, 2019, p. 186).

(2010) argumentam que não se trata da *restrição* dos fluxos de informação: é preciso assegurar um fluxo *apropriado*. Deve-se produzir soluções baseadas em contexto (*context-based*); a depender do tipo de informação coletada, do ator que a coleta e do uso adotado, são usadas diferentes técnicas e políticas (NISSENBAUM, 2010, p. 1-2; 219-20).

O Facebook, por exemplo, após ser alvo de diversos protestos quanto ao seu modelo de operação, respondeu conferindo maior controle aos usuários sobre a informação disponível em seus perfis. Contudo, essa solução não resolve o problema da privacidade. É preciso, além disso, contestar a lógica disseminada pelo capitalismo de vigilância de que informações compartilhadas são públicas, podem ser apropriadas por qualquer um, que é a principal premissa de empresas como Google e Facebook. A depender de quem recebe uma informação, mais ou menos poder este tem sobre o titular: alguns podem infligir danos ou constrangimento, oferecer oportunidades importantes ou até orientar decisões (NISSENBAUM, 2010, p. 216; 228).

Este trabalho se dedicou a destacar as consequências que as assimetrias de poder do capitalismo de vigilância impõem sobre a privacidade, mas também sobre o exercício da democracia. À medida que se sabe tanto sobre nós e a principal forma como adquirimos conhecimento é controlada por algumas empresas, somos feitos reféns. E quem vai nos salvar?

Com o Estado muitas vezes incentivando ou inconsciente das práticas perpetuadas pelas *big tech* e estas pouco interessadas em mudar seu modelo de negócios tão lucrativo, cabe a nós a responsabilidade de nos libertar das amarras impostas pelo capitalismo de vigilância. Precisamos nos organizar em movimentos estudantis, institutos de pesquisa e grupos de ativismo para, em primeiro lugar, expor os problemas do capitalismo de vigilância, e exigir a garantia da privacidade e que sejam impostos limites e controles sobre o setor privado. O futuro está em risco, quem vai defendê-lo?

Bibliografia

ABU-LABAN, Yasmeen. The politics of surveillance: Civil liberties, human rights and ethics. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 420-427.

AGAR, Jon. *The Government Machine*: A Revolutionary History of the Computer, Cambridge: MIT Press, 2003. p. 554.

ALLCOTT, Hunt; GETZHOW, Matthew. Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives*, v. 31, n. 2, 2017. p. 211–236. https://doi.org/10.1257/jep.31.2.211 doi=10.1257/jep.31.2.211

ALMEIDA, Virgílio A. F., et al. Governance Challenges for the Internet of Things. *IEEE Internet Computing*, v. 19, n. 4, pp. 56-59, jul-ago. 2015, doi: 10.1109/MIC.2015.86.

ALMEIDA, Virgílio A. F.; DONEDA, Danilo. O que é governança de algoritmos? *PoliTICS*, out. 2016. Disponível em: <https://politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos>. Acesso: 02 set. 2020.

ANGWIN, Julia et al. Facebook Enabled Advertisers to Reach 'Jew Haters', *ProPublica*, 14 set 2017. Disponível em: <https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters>. Acesso em: 12 set 2020.

BARRÍA, Cecília. As cinco piores bolhas da história da economia – e por que elas ainda assustam. *BBC*, 23 dez. 2017. Disponível em: <https://www.bbc.com/portuguese/geral-42418028>. Acesso em: 23 ago. 2020.

BENNETT, Colin. Privacy advocates, privacy advocacy and the surveillance society. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 412-419.

BENTES, Anna. A Gestão Algorítmica da Atenção: enganchar, conhecer e persuadir. In: POLIDO, Fabrício; ANJOS, Lucas; BRANDÃO, Luíza (orgs.), *Políticas, internet e sociedade*. Belo Horizonte: IRIS – Instituto de Referência em Internet e Sociedade, 2019. Disponível em: http://bit.ly/35hiqms. Acesso em: 05 set. 2020.

BIRKBAK, Andreas; CARLSEN, Hjalmar Bang. The Public and its Algorithms: Comparing and experimenting with calculated publics. In: AMOORE, Louise; PIOTUKH, Volha (eds.). *Algorithmic Life*: Calculative devices in the age of big data. New York: Routledge, 2016, p. 37-53.

BROUSSARD, Meredith. *Artificial unintelligence*: How computers misunderstand the world. Cambridge: MIT Press, 2018. 248 p.

BROWN, Abram. Discord Was Once The Alt-Right's Favorite Chat App. Now It's Gone Mainstream And Scored A New $3.5 Billion Valuation. *Forbes*, 30 jun. 2020. Disponível em: <https://www.forbes.com/sites/abrambrown/2020/06/30/discord-

was-once-the-alt-rights-favorite-chat-app-now-its-gone-mainstream-and-scored-a-new-35-billion-valuation/>. Acesso em 15 out. 2020.

BROWNE, Simone. Race and surveillance. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 72-79.

BRUNO, Fernanda. A Economia Psíquica dos Algoritmos: Quando o Laboratório É o Mundo. *Jornal NEXO*. Disponível em: <https://www.nexojornal.com.br/ensaio/2018/A-economia-ps%C3%ADquica-dos-algoritmos-quando-o-laborat%C3%B3rio-%C3%A9-o-mundo>. Apud BENTES, Anna. A Gestão Algorítmica da Atenção: enganchar, conhecer e persuadir. In: POLIDO, Fabrício; ANJOS, Lucas; BRANDÃO, Luíza (Orgs.), *Políticas, internet e sociedade*. Belo Horizonte: IRIS – Instituto de Referência em Internet e Sociedade, 2019. Disponível em: http://bit.ly/35hiqms. Acesso em: 05 set. 2020.

_____. *Máquinas de ver, modos de ser*: vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 2013. 190 p.

_____. Surveillance and participation on Web 2.0. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 343-351.

BRUNTON, Finn; NISSENBAUM, Helen. *Obfuscation*: A User´s Guide for Privacy and Protest. Nova York: MIT Press, 2015. 136 p.

CASTELLS, Manuel. *A Sociedade em Rede*; tradução: Roneide Venâncio Majer. 6ª ed. São Paulo: Paz e Terra, 1999. 698 p.

CEYHAN, Ayse. Surveillance as biopower. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 38-45.

CLOUD, Morgan. Property is Privacy: Locke and Brandeis in the Twenty-First Century. *American Criminal Law Review*, v. 55, n. 37, 2018.

COHEN, Julie. Examined Lives: Informational Privacy and the Subject as Object. *Stanford Law Review*, v. 52, p. 1373–1437, 2000.

COHEN, Nicole S. The Valorization of Surveillance: Towards a Political Economy of Facebook. *Democratic Communiqué*, v. 22, n. 1, Spring 2008.

D'ALESSANDRO, Brian et al. Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification. *Big Data*, v. 5, n. 2, 2017, p. 120-134. Disponível em: <https://arxiv.org/abs/1907.09013>. Acesso em 14 set 2020.

DEIBERT, Ronald J. Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs*, v. 32, n. 4, 2018, pp. 411–424.

DEVILLE, Joe; VAN DER VELDEN, Lonneke. Seeing the Invisible Algorithm: The practical politics of tracking the credit trackers. In: AMOORE, Louise; PIOTUKH, Volha (eds.). *Algorithmic Life: Calculative devices in the age of big data*. New York: Routledge, 2016. p. 122-147.

DIAS, Tatiana. ‘O dilema das redes': sair da internet não vai salvar a internet. *The Intercept Brasil*, 14 set. 2020. Disponível em: <https://theintercept.com/2020/09/14/internet-netflix-redes/>. Acesso em: 27 set. 2020.

DILEMA das Redes. Direção: Jeff Orlowski. Estados Unidos: Netflix, 2020 (89 min.).

DIRESTA, Renée. AI-Generated Text Is the Scariest Deepfake of All. *Wired*, 31 jul. 2020. Disponível em: <https://www.wired.com/story/ai-generated-text-is-the-scariest-deepfake-of-all/>. Acesso em 14 set 2020.

_____. The Return of Fake News—and Lessons From Spam, *Wired*, 05 jun. 2019. Disponível em: <https://www.wired.com/story/the-return-of-fake-news/>. Acesso em 14 set. 2020.

_____. The Information War Is On. Are We Ready For It?, *Wired*, 03 ago. 2018. Disponível em: <https://www.wired.com/story/misinformation-disinformation-propaganda-war/>. Acesso em 14 set. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Revista Espaço Jurídico*, v. 12, n. 2, p. 91-108, jul./dez. 2011.

_____. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. 352 p.

EISENSTAT, Yael. Dear Facebook, this is how you’re breaking democracy. *TED*, ago. 2020. Disponível em: <https://www.ted.com/talks/yael_eisenstat_dear_facebook_this_is_how_you_re_breaking_democracy/transcript. Acesso em: 27 set. 2020.

FINN, Ed. *What Algorithms Want*: Imagination in the Age of Computing. Cambridge: MIT Press, 2017. 272 p.

FISCHER, Sara. Facebook threatens to pull news from Australia if new law passes, *Axios*, 1 set. 2020. Disponível em: <https://www.axios.com/facebook-pull-australia-news-threat-new-law-8615dab5-59e7-4683-80cd-3f2254d8faba.html?utm_source=meio&utm_medium=email>. Acesso em 12 set 2020.

FOUCAULT, Michel. *Security, Territory, Population*: Lectures at the Collège de France. Senellard, Michel; Ewald, François; Fontana, Alessando (eds.). Basingstoke: Palgrave Macmillan, 2007. 436 p.

FRIEDEWALD, Michael et al. *Surveillance, Privacy and Security*: Citizens’ Perspectives. New York: Routledge, 2017. 310 p.

FÜHRDING, Steffen. Religion, Privacy and the Rise of the Modern State. *Method and Theory in the Study of Religion*, v. 25, 2013. p. 118-131.

GIDDENS, Anthony. *The Consequences of Modernity*, Cambridge: Polity, 1990. 186 p.

GILLINGS, Martin R. et al. Information in the Biosphere: Biological and Digital Worlds. *Trends in Ecology and Evolution*, v. 31, n. 3, mar. 2016.

GILLIOM, John; MONAHAN, Torin. Everyday resistance. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 405-411.

_____. *SuperVision:* An Introduction to the Surveillance Society. Chicago: University of Chicago, 2013. 200 p.

GLASER, April. The Watchdogs That Didn't Bark. *Slate*, 19 abr. 2018. Disponível em: <https://slate.com/technology/2018/04/why-arent-privacy-groups-fighting-to-regulate-facebook.html>. Acesso em: 15 set 2020.

HARRIS, Tristan. Technology Platforms Must Operate for the Public Good. *Milken Institute*, 22 abr. 2020. Disponível em: <https://milkeninstitute.org/power-of-ideas/technology-platforms-must-operate-public-good>. Acesso em 15 out. 2020.

HOPKINS, Nick. Revealed: Facebook's internal rulebook on sex, terrorism and violence. *The Guardian*, 21 mai. 2017. Disponível em: < https://www.theguardian.com/news/2017/may/21/revealed-facebook-internal-rulebook-sex-terrorism-violence?>. Acesso em: 12 ago. 2020.

HUREL, Louise Marie. *Cybersecurity and Internet Governance*: Two Competing Fields? Monografia (Graduação em Relações Internacionais) - Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), 2016.

IBM CEO's Letter to Congress on Racial Justice Reform. *IBM THINK Policy Blog*, 8 jun. 2020. Disponível em: <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>. Acesso em: 15 out. 2020.

JENKINS JR, Holman W. Google and the Search for the Future, *The Wall Street Journal*, 14 ago. 2010. Disponível em: < https://www.wsj.com/articles/SB10001424052748704901104575423294099527212>. Acesso em: 30 ago. 2020.

KAK, Amba; RICHARDSON, Rashida. Artificial Intelligence Policies Must Focus on Impact. *Centre for International Governance Innovation*, 1 mai. 2020. Disponível em: <https://www.cigionline.org/articles/artificial-intelligence-policies-must-focus-impact-and-accountability>. Acesso em 12 set. 2020.

KANTROWITZ, Alex. Google Allowed Advertisers To Target People Searching Racist Phrases, *BuzzFeed News*, 15 set. 2017. Disponível em: <https://www.buzzfeednews.com/article/alexkantrowitz/google-allowed-advertisers-to-target-jewish-parasite-black>. Acesso em: 12 set 2020.

KERR, Ian; BARRIGAR, Jennifer. Privacy, identity and anonymity. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 386-394.

KOSKELA, Hille. "You shouldn't wear that body": surveillance and gender. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 49-56.

LANCHESTER, John. Você é o produto: Mark Zuckerberg e a colonização das redes pelo Facebook. *Revista Piauí*, ed. 132, set 2017. Disponível em: <https://piaui.folha.uol.com.br/materia/voce-e-o-produto/>. Acesso: 20 mai. 2020.

LANIER, Jaron; EUCHNER, Jim. What Has Gone Wrong with the Internet, and How We Can Fix It. *Research-Technology Management*, mai-jun 2019, p. 13-9.

LEAVY, Edward Harrison. *Technopopulism*: Movimento Cinque Stelle, Podemos, And the Rise of Digital Direct Democracy. 2018. Tese (Mestrado em Artes pelo Departamento de Ciência Política) - University of North Carolina at Chapel Hill, Chapel Hill, 2018.

LESSA, Renato. Representação Política: Fundamentos e Dilemas. *Palestra Fórum Senado Brasil*, 27 jun. 2012. Disponível em: <https://youtu.be/-49FwCJTYFU>. Acesso 26 set 2020.

LEWIS, Paul. 'Our minds can be hijacked': The Tech Insiders Who Fear a Smartphone Dystopia. *The Guardian*, 6 out. 2017. Acesso em: <https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia>. Acesso em: 12 ago. 2020.

LOPES, André. FaceApp volta a viralizar em 2020 e reacende preocupação com a privacidade. *Veja*, 15 jun 2020. Disponível em: <https://veja.abril.com.br/tecnologia/faceapp-volta-a-viralizar-em-2020-e-reacende-preocupacao-com-a-privacidade/>. Acesso em: 06 jul 2020.

LYON, David. Surveillance after September 11. *Sociological Research Online*, v. 6, n. 3, 30 nov. 2001. Disponível em: <http://www.socresonline.org.uk/6/3/lyon.html>. Acesso em: 14 ago. 2020.

MAGRANI, Eduardo. Threats of the Iot in a Techno-regulated Society – a new legal challenge of the information revolution. *The ORBIT Journal*, v. 1, n. 1, 2017, p. 1-17.

MILL, John Stuart. *On Liberty*. Kitchener: Batoche Books, 2001. 109 p.

MOROZOV, Evgeny. Digital Socialims: Reimagining social democracy for the 21st century. *Eurozine*, 21 fev. 2020. Disponível em: <https://www.eurozine.com/digital-socialism/>. Acesso em: 13 jul. 2020.

_____. There's only one way to take on big tech: by reining in big money and big state. *The Guardian*, 28 nov. 2019. Disponível em: < https://www.theguardian.com/commentisfree/2019/nov/28/big-tech-populist-stance-big-money-big-state>. Acesso em: 13 jul. 2020.

_____. The Real Privacy Problem. *MIT Technology Review*, 22 out. 2013. Disponível em: <https://www.technologyreview.com/2013/10/22/112778/the-real-privacy-problem/>. Acesso em: 13 jul. 2020.

MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a Tutela de Direitos Fundamentais: Uma Análise à Luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

_____. Mercado, pessoa humana e tecnologias: a Internet das Coisas e a proteção do direito à privacidade. In: Marcos Ehrhardt Júnior; Eroulths Cortiano Junior. (Org.). *Transformações no Direito Privado nos 30 anos da Constituição*: estudos em homenagem a Luiz Edson Fachin. 1ed.Belo Horizonte: Forum, 2019, v. 1, p. 103-115.

NISSENBAUM, Helen. *Privacy in Context:* Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books, 2010. 288 p.

NOBLE, Safiya Umoja. *Algorithms of oppression*: How search engines reinforce racism. NYU Press, 2018. 256 p.

PENNEY, Jonathon, et al. Advancing Human-Rights-By-Design in the Dual-Use Technology Industry. *Journal of International Affairs*, v. 71, n. 2, 2018, pp. 103–110.

PETERS, Jay. IBM will no longer offer, develop, or research facial recognition technology. *The Verge*, 8 jun. 2020. Disponível em: <https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software>. Acesso em: 15 out. 2020.

PRIVACIDADE (Temporada 2). *Expresso Futuro*. Apresentação: Ronaldo Lemos. Rio de Janeiro: TV Futura, 2018. Disponível em: <http://www.futuraplay.org/video/privacidade/434980/>. Acesso em: 30 set. 2019.

PRZEWORSKI, Adam. Ama a Incerteza e Serás Democrático. *Novos Estudos*, n. 9, jul. 1984, p. 36- 46.

QUEIMALIÑOS, Rebeca. Sleeping Giants: O homem que arruinou a extrema direita nos EUA. *ICON/EL País Brasil*, 17 mai. 2020. Disponível em: < https://brasil.elpais.com/icon/2020-05-17/o-homem-que-arruinou-a-extrema-direita-nos-eua.html>. Acesso em: 13 jun. 2020.

RAYNES-GOLDIE, Kate. the political economy of facebook (or, why we hate facebook but keep using it). *Dr. Kate's blog*, 7 mai. 2007. Disponível em: < http://www.k4t3.org/2007/05/07/the-political-economy-of-facebook-or-why-we-hate-facebook-but-keep-using-it/>. Acesso em: 21 out. 2020.

REGAN, Julia. Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill & London: The University of North Carolina Press, 1995. 310 p.

REGAN, Priscilla. Regulating surveillance technologies: Institutional arrangements. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 397-404.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 381.

RULE, James. "Needs" for surveillance and the movement to protect privacy. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 64-71.

SARTORI, Giovanni. *Teoria da democracia revisitada*. São Paulo: Ed. Ática, 1994. 240 p.

SHAW, Jonathan. The Watchers: Assaults on privacy in America, jan-fev. 2017, *Harvard Magazine*. Disponível em: <https://harvardmagazine.com/2017/01/the-watchers>. Acesso em: 10 jul. 2019.

SILVA, Tarcízio. Racismo Algorítmicos em Plataformas Digitais: Micro agressões e Discriminação em Código. In: SILVA, Tarcízio (Org.). *Comunidades,*

Algoritmos, Algoritmos e Ativismos Digitais: Olhares Afrodiaspóricos. São Paulo: 2020. p. 120-137.

SOLOVE, Daniel. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, v. 154, n. 3, jan 2006.

STEEVES, Valerie. Hide and seek: Surveillance of young people on the internet. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 352-359.

STRANDBURG, Katherine J. Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context. In: LANE, Julia; STODDEN, Victoria; BENDER, Stefan; NISSENBAUM, Helen (Eds.), *Privacy, Big Data, and the Public Good*: Frameworks for Engagement. Cambridge: Cambridge University Press, 2014. p. 5-43.

TENENTE, Luiza. 30% dos domicílios no Brasil não têm acesso à internet; veja números que mostram dificuldades no ensino à distância, *G1*, 26 mai. 2020. Disponível em: <https://g1.globo.com/educacao/noticia/2020/05/26/66percent-dos-brasileiros-de-9-a-17-anos-nao-acessam-a-internet-em-casa-veja-numeros-que-mostram-dificuldades-no-ensino-a-distancia.ghtml>. Acesso em: 02 nov. 2020.

VAN OTTERLO, Martijn. The Libraryness of Calculative Devices: Artificially Intelligent Librarians and Their Impact on Information Consumption. In: AMOORE, Louise; PIOTUKH, Volha (eds.). *Algorithmic Life*: Calculative devices in the age of big data. New York: Routledge, 2016, p. 54-81.

WAKEFIELD, Jake. Zoom boss apologizes for security issues and promises fixes. *BBC*, 02 abr. 2020. Disponível em: <https://www.bbc.com/news/technology-52133349>. Acesso em: 08 ago. 2020.

WARREN, Samuel D. & BRANDEIS, Louis D.. The Right to Privacy. *Harvard Law Review*, v. 4, n. 5, 5 dez, 1890. p. 193-220. Disponível em: <http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C>. Acesso em: 21 jun 2020.

WATSON, Chloe. The key moments from Mark Zuckerberg's testimony to Congress. *The Guardian*, 11 abr. 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments>. Acesso em: 23 out. 2020.

WELLER, Toni. The information state: An historical perspective on surveillance. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies.* New York: Routledge, 2012. p. 57-63.

WESTIN, Alan. *Privacy and Freedom*. Nova York: Ig Publishing, 2018. ISBN: 978-1-63246-073-8 (ebook).

WHITMANT, James Q.. The Two Western Cultures of Privacy: Dignity Versus Liberty. *The Yale Law Journal*, v. 113, n. 1151, 2004.

WOOD, David Murakami. Globalization and surveillance. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David (eds.). *Routledge Handbook of Surveillance Studies*. New York: Routledge, 2012. p. 333-342.

WU. Tim. *Impérios da Comunicação*: Do telefone à internet, da AT&T ao Google. Rio de Janeiro: Zahar, 2012. 483 p.

_____. The Attention Merchants: The Epic Scramble to Get Inside our Heads. New York: Knopf, 2016. 403 p.

ZICARI, Roberto V. Defining global digital ethics standards. *Harvard Business School Digital Initiative*, 9 abr. 2019. Disponível em: <https://digital.hbs.edu/data-and-analysis/on-european-data-protection-interview-with-giovanni-buttarelli/>. Acesso em: 16 mai. 2020.

ZUBOFF, Shoshana. Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação. In.: CARDOSO, Bruno et al. *Tecnopolíticas da vigilância:* Perspectivas da margem. São Paulo: Boitempo, 2018, p. 17 - 68.

_____. *The Age of Surveillance Capitalism*: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019. 704 p.