UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE CIÊNCIAS E LETRAS – FCL/AR – CAMPUS ARARAQUARA
PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIAS SOCIAIS

JUAN FELIPE DO PRADO ALVES

OS LIMITES DA CAPITALIZAÇÃO DE DADOS: O CAPITALISMO DE VIGILÂNCIA E A LEI 13.709/2018

ARARAQUARA-SP

2025

JUAN FELIPE DO PRADO ALVES

OS LIMITES DA CAPITALIZAÇÃO DE DADOS: O CAPITALISMO DE VIGILÂNCIA E A LEI 13.709/2018

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Ciências Sociais, junto ao Programa de Pós-Graduação em Ciências Sociais, da Faculdade de Ciências e Letras da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Araraquara.

Linha de Pesquisa: Estado, Instituições e Políticas Pública
Orientadora: Professora Doutora Carla Gandini Giani Martelli

Araraquara
2025

A474l

Alves, Juan Felipe do Prado
OS LIMITES DA CAPITALIZAÇÃO DE DADOS : O CAPITALISMO DE VIGILÂNCIA E A LEI 13.709/2018 / Juan Felipe do Prado Alves. -- Araraquara, 2025
94 p.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências e Letras, Araraquara
Orientadora: Carla Gandini Giani Martelli

1. capitalismo de vigilância. 2. neoliberalismo. 3. democracia. 4. colonialismo de dados. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

JUAN FELIPE DO PRADO ALVES

OS LIMITES DA CAPITALIZAÇÃO DE DADOS: O CAPITALISMO DE VIGILÂNCIA E A LEI 13.709/2018

Dissertação de mestrado apresentada à Universidade Estadual Paulista (UNESP), FCL/ar, Araraquara, para obtenção do título Mestre em Ciências Sociais.

Linha de Pesquisa: Estado, Instituições e Políticas Públicas

Data da defesa: 18/02/2025

Banca Examinadora:

_____
Prof. Dra. Carla Gandini Giani Martelli
UNESP - FCLAR- Campus de Araraquara

_____
Prof. Dr. Marcelo Santos
UNESP- FCLAR- Campus de Araraquara

_____
Prof. Dr. Alessandra Santos Nascimento
UNIARA

AGRADECIMENTOS

Agradeço imensamente à minha família, por me apoiar em todos os momentos em minha jornada, e a minha companheira Julia, por estar sempre a meu lado. Agradeço também à professora Carla, por todo o suporte na elaboração desta pesquisa, e a todos os outros professores que participaram de minha formação.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001

“O social dá lugar ao sozinho. Não a multidão, mas sim a solidão caracteriza a constituição social atual” (Byung-Chul Han, 2018, p. 33).

RESUMO

Em diálogo com reflexões teóricas sobre o conceito de liberdade e o neoliberalismo, o objetivo geral do presente trabalho é trazer reflexões sobre as transformações sociais, políticas e econômicas causadas pelas grandes empresas de tecnologia, chamadas Big Techs, e suas tecnologias voltadas à coleta, ao acúmulo e à comercialização de dados sobre as pessoas no mundo todo. Como objetivo específico, investigou-se o alcance da Lei Geral de Proteção de Dados (LGPD) para limitar e/ou potencializar o chamado "capitalismo de vigilância" no Brasil. Tal análise da lei se deu a partir dos aspectos fundamentais do capitalismo de vigilância, os quais foram apresentados no momento anterior à análise. A pesquisa permitiu concluir que, ainda que a Lei Geral de Proteção de Dados avance na proteção de direitos dos cidadãos ao exigir o consentimento dos titulares de dados para a coleta de seus dados, há limites na regulamentação que deixam a população vulnerável em relação ao poder das Big Techs em monitorar e manipular dados com impactos importantes para vários aspectos da vida em sociedade e para os sistemas democráticos. O estudo ainda concluiu que é preciso instruir e educar a população sobre os problemas e consequências advindos da ampla circulação de tecnologias de vigilância.

Palavras-Chave: Capitalismo de vigilância; neoliberalismo; democracia; colonialismo de dados.

ABSTRACT

In dialogue with theoretical reflections on the concept of freedom and neoliberalism, the general objective of this work is to bring reflections on the social, political and economic transformations caused by large technology companies, called Big Techs, and their technologies aimed at collecting, accumulating and commercializing data on people around the world. As a specific objective, we investigated the scope of the Lei Geral de Proteção de Dados(LGPD) to limit and/or enhance the so-called “surveillance capitalism” in Brazil. This analysis of the law was based on the fundamental aspects of surveillance capitalism, which were presented prior to the analysis. The research concluded that, although the General Data Protection Law advances the protection of citizens' rights by requiring the consent of data subjects for the collection of their data, there are limits in the regulation that leave the population vulnerable to the power of Big Tech to monitor and manipulate data with important impacts on various aspects of life in society and on democratic systems. The study also concluded that the population needs to be educated about the problems and consequences of the wide circulation of surveillance technologies.

Keywords: surveillance capitalism; neoliberalism; democracy; data colonialism

SUMÁRIO

1.INTRODUÇÃO 9

1.2 REFERENCIAL TEÓRICO-METODOLÓGICO 11

2. CAPITALISMO DE VIGILÂNCIA, BIG TECHS E COLONIALISMO DE DADOS 19

2.1 SOCIEDADE DISCIPLINAR E SOCIEDADE DE CONTROLE 22

2.2 OS NOVOS IMPERATIVOS DO CAPITALISMO DE VIGILÂNCIA 28

2.3 DIVISÃO DA APRENDIZAGEM 30

2.4 MODULAÇÃO COMPORTAMENTAL/ ALGORITMOS 30

2.5 CONTRATOS E INCONTRATOS 33

3. NEOLIBERALISMO E CAPITALISMO DE VIGILÂNCIA 38

3.1 LAÇOS DE COLONIALIDADE 40

3.2 O MERCADO DE DADOS E A VENDA DE DEMOCRACIA 43

3.3 RELAÇÕES DE PODER E DOMINAÇÃO 47

4. A LEI 13.709/2018, CONTEXTO E IMPLICAÇÕES 51

4.1 CONTEXTO DE APROVAÇÃO DA LGPD 52

4.2 MÉTODO DE ANÁLISE DA LEI 13.709/2018 (LGPD) 53

4.3 DISPOSIÇÕES PRELIMINARES DA LGPD 55

4.4 LGPD E OS LIMITES DO CAPITALISMO DE VIGILÂNCIA 56

4.5 ARTIGO 10º E O PROBLEMA DO LEGÍTIMO INTERESSE 65

4.6 A ANONIMIZAÇÃO DE DADOS 69

4.7. A LGPD E AS PEQUENAS E MICRO EMPRESAS 72

5. A LGPD NA RELAÇÃO ENTRE EMPRESAS E CIDADÃOS 74

5.1 AS FUNÇÕES DA LGPD 74

5.2 A LGPD E A EXPLORAÇÃO BIG TECHS/CIDADÃOS 75

6. CONSIDERAÇÕES FINAIS 79

REFERÊNCIAS 84

1.**INTRODUÇÃO**

Os aparelhos digitais que permitem ampla comunicação são objeto de estudo de diversas ciências desde que surgiram, pois foram fundamentais para uma ampla transformação social e transnacional, encurtando barreiras fronteiriças, permitindo compartilhamento massivo de informação que são acessíveis a preços relativamente convenientes para muitas pessoas, visto que qualquer pessoa com um celular que tenha acesso a internet já estará integrada a rede mundial de computadores. Não sem motivo muitas pessoas, incluindo muitos pesquisadores, criaram visões um tanto otimistas sobre esse novo momento social sustentado com a ampliação de novas tecnologias cada vez mais inovadoras, que permitiram pensar sobre democracia digital, democratização do conhecimento, e uma série de outras potências que os novos aparelhos apresentavam e que pareciam ser muito bem vindos a qualquer pensador social comprometido com valores democráticos. No entanto, muito deste otimismo foi substituído por uma preocupação: os ambientes digitais são amplamente pautados por fundamentos e atores do mercado, sendo assim, os fundamentos da democracia não são parte estruturante desta relação entre usuários e máquina, mas sim imperativos do mercado: lucro, venda, consumo e outros.

Pode-se dizer que a lógica mercadológica está posta na própria estrutura das redes como se apresentam, e que, sendo assim, seja preciso estabelecer como opera de fato essa estrutura e como ela afeta as sociedades. Shoshana Zuboff (2021) foi uma das principais pensadoras a contribuir com o entendimento sobre este assunto, e por isso será a principal referência ao se tratar de capitalismo de vigilância, conceito tão importante hoje para se tratar de estudos referentes ao digital. Como ficará evidente ao longo da pesquisa, a intenção não é problematizar os aparelhos tecnológicos em si, mas sim a função a qual lhes foi atribuído: não como ferramentas para a solução de problemas, mas como tecnologias de vigilância, que foram fundamentais para a solidificação do capitalismo de vigilância. Esta forma de capitalização se sustenta a partir de uma profunda desigualdade entre os países, o que permite um cenário de expressiva exploração entre os países em que as empresas de vigilância estão sediadas e os demais. Será apresentado ao longo do trabalho como essas desigualdades significam relações de dependência dos países vigiados em relação às empresas vigilantes, e como este cenário é fortalecido e fortalece as relações de colonialidade no século XXI.

Este novo modelo econômico causou efeitos diretos no Brasil, e coube então ao poder público brasileiro elaborar políticas de regulação sobre o capitalismo de vigilância. Esta pesquisa tem como foco estudar a lei 13.709/2018, conhecida como LGPD, por entender que

esta trata do limite entre o que pode ou não ser coletado por empresas, o que atinge diretamente a operação da capitalização de dados. Nesse sentido, uma análise documental desta lei se justifica na medida em que se relaciona diretamente ao capitalismo de vigilância e as problemáticas sociais levantadas por ele. O objetivo é entender como a LGPD opera sobre as relações de poder estabelecidas entre as grandes empresas de tecnologia e os usuários brasileiros.

Assume-se a definição de capitalismo de vigilância dada por Zuboff, pois ela permite estudar o desenvolvimento do mercado mundial de dados e suas investidas contra a privacidade dos indivíduos, a qual é compreendida como a capacidade das pessoas de definir o que será compartilhado, e contra as instituições democráticas destes países, causando consequências diversas e amplas sobre resultados eleitorais, por exemplo. O capitalismo de vigilância é, certamente, um fenômeno central para que se entenda os cenários políticos do século XXI, sendo também profundamente complexo por abranger diversos países e ser consequência de relações de poder muito anteriores ao tempo presente. Posta esta complexidade, esta pesquisa se atém ao que se considera fundamental a este fenômeno, isto é, o que se entende por capitalismo de vigilância neste momento não pode ser entendido separado do: acúmulo ilimitado de dados; capitalização de dados; integração das tecnologias de vigilância da sociedade como um todo; incontrato; colonialismo de dados; divisão desigual da aprendizagem e cidades inteligentes. Cada uma destas partes fundantes do capitalismo de vigilância será contemplada no decorrer na pesquisa, de forma a fazer entender a importância de cada uma para a sustentação e disseminação desta forma de capitalização.

Este texto foi organizado em sete seções, além desta introdução, cada uma delas constituindo de uma a cinco subseções além desta introdução. Na segunda, serão evidenciados os referenciais teóricos e a metodologia aplicada para a elaboração desta dissertação, após isso, se explicitará os principais conceitos fundamentais para esta pesquisa, tais quais capitalismo de vigilância, Big Techs e colonialismo de dados. Em um terceiro momento da pesquisa, se discutirá sobre neoliberalismo, conceito importante nas ciências sociais e que permite entender o cenário político e econômico no qual se desenvolve o capitalismo de vigilância. Na quarta seção se iniciará a apresentação da lei 13.709/2018, incluindo seu histórico formativo, sua justificativa, e a forma com a qual tal lei será analisada. Na quinta seção se discutirá propriamente sobre como a lei 13.709/2018 se relaciona com as pequenas empresas, que também precisam se adaptar às novas regras. Na sexta seção será ponderado de que forma e em que medida a lei analisada interage com o capitalismo de vigilância. A sétima seção dedica-se

às considerações finais, em que se elabora a conclusão desta pesquisa, retomando o que foi exposto ao longo dela. Por fim estarão dispostas as referências bibliográficas que permitiram a elaboração desta pesquisa.

1.2 Referencial teórico-metodológico

Esta pesquisa se desenvolveu a partir de um diálogo com autores clássicos, como John Stuart Mill (2011), John Locke (2020) e Foucault (1975), e autores contemporâneos, como Shoshana Zuboff (2021), Wendy Brown (2019) e Evgeny Morozov (2018). Acredita-se que tais autores permitam a elaboração de uma reflexão aprofundada sobre o tema da liberdade, tão caro a esta pesquisa, além de permitir que esta pesquisa contemple pesquisas recentes sobre as novas tecnologias e as diversas consequências que elas apresentam. Além do diálogo com a teoria, a pesquisa investigou a Lei 13.709/2018, que foi uma importante iniciativa do governo federal brasileiro para estabelecer os limites da captura e o acúmulo de dados por empresas[1]. Para a análise da lei foram detalhados seus artigos, dando especial atenção aos que dialogam mais diretamente com o capitalismo de vigilância e seus mecanismos, de forma que se permitisse entender a relação entre o capitalismo de vigilância e a lei analisada. Anteriormente à redação deste texto, foi feita uma pesquisa para que se pudesse conhecer quais autores estavam discutindo o tema e quais obras foram publicadas que pudessem garantir profundidade a discussão elaborada. Tal pesquisa prévia utilizou-se de sites de busca acadêmicos amplamente reconhecidos, como Google Acadêmico e Scielo. Sem a pretensão de abarcar todos os autores nem todas as obras que se relacionassem ao tema desta pesquisa, acredita-se que autores relevantes da discussão foram contemplados.

Esta pesquisa é de caráter qualitativo, e não contempla análise empírica ou de dados quantitativos, mas contempla análise qualitativa e documental da lei 13.709/2018, não apenas a partir da leitura de seus artigos e da interpretação deles, mas também a partir de autores que se propuseram a investigar também esta lei e elaborar conclusões sobre ela. Além disso, os impactos da lei sobre a LGPD foram compreendidos à luz das características entendidas como fundamentais ao capitalismo de vigilância. No decorrer da pesquisa, percebeu-se a necessidade de integrar o debate em torno de colonialismo de dados, muito associado ao capitalismo de vigilância. Tal debate foi integrado a partir de pesquisas que tratassem do tema.

[1] A lei em questão pode ser lida em sua versão mais recente através do site: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Uma questão posta no século XXI, apesar de não ter surgido nele, é sobre os limites das grandes empresas de tecnologia (as chamas Big Techs) em nossas vidas. Aparelhos como celulares, computadores, *notebooks* entre outros, fazem parte do dia a dia dos cidadãos (e com cada vez mais intensidade) nos mais diversos países, e as Big Techs assumem cada vez mais espaço na vida das pessoas a partir destes aparelhos. Com esta realidade de expansão de poder empresarial das Big Techs, qual seria a melhor forma de definir as fronteiras sobre como essas empresas podem agir nas vidas das pessoas?

A preocupação sobre os limites da liberdade e da privacidade não são de hoje, há séculos a humanidade questiona até que ponto uma pessoa ou um grupo delas pode decidir o que fazer a partir de seus desejos. Muitos autores consagrados do século XVIII procuraram contribuir com essa discussão. Stuart Mill (2011), por exemplo, trabalhou para estabelecer de forma lógica um limite à interferência do Estado, e dos cidadãos, à vida alheia. Para o autor, toda a interferência sobre assuntos que apenas ao indivíduo dizem respeito são ilegítimas, mantendo-se algumas exceções, como no caso de indivíduos que não estão com suas faculdades mentais a plena disposição (como crianças ou pessoas deficientes mentais, por exemplo). Nas palavras do autor:

> Os assuntos que só ao próprio dizem respeito são, por excelência, os que dizem respeito aos sentimentos e opiniões das pessoas, aos seus gostos e objetivos na vida, e à associação voluntária de pessoas — que sejam maiores de idade e estejam em plena posse das suas faculdades mentais — para objetivos que não impliquem dano a outros (MILL, 2011, p.10).

A definição de Mill estabelece então um limite ao poder dos que o têm em abundância, sejam pessoas, grupos ou o Estado. Para o autor, o que apenas diz respeito a um indivíduo não deverá sofrer interferências vindas de outro. É em defesa das liberdades individuais e contra toda a forma de interferência na vida privada dos indivíduos, seja por parte do Estado, seja por parte da própria sociedade, que se coloca Stuart Mill. De fato, quando Mill reflete sobre as questões da liberdade, está bastante preocupado com como o Estado deve agir em relação aos cidadãos, já que a disparidade de poder entre o Estado e o indivíduo faz com que seja muito importante definir como o primeiro pode agir em relação ao segundo, mas, como antes dito, não é apenas sobre o Estado de seu tempo que Mill reflete, o que permite que suas conclusões sejam importantes contribuições para pensarmos a liberdade até os dias de hoje. As Big Techs, por exemplo, como se poderá perceber no decorrer da pesquisa, não assumem com muita exatidão o limite de liberdade proposto pelo autor, ou, ao menos, não o respeitam.

Stuart Mill passou por formação filosófica utilitarista, a qual busca compreender a forma com a qual os indivíduos, em plenas capacidades racionais, tomam suas decisões. Tal filosofia parte do princípio de que os sujeitos tomam suas decisões com base na satisfação que tais ações lhes serão geradas, isto é, a escolha que for mais vantajosa a quem escolhe, tende a ser a escolhida:

> Por princípio de utilidade entende-se aquele princípio que aprova ou desaprova qualquer ação, segundo a tendência que tem a aumentar ou diminuir a felicidade da pessoa cujo interesse está em jogo, ou, o que é a mesma coisa em outros termos, segundo a tendência a promover ou a comprometer a referida felicidade (BENTHAM, p.10, 1974)

Isto quer dizer que há um cálculo voltado ao interesse pessoal para a tomada de decisão, feito, evidentemente, a partir dos conhecimentos prévios do decisor. Para que os indivíduos possam praticar suas escolhas nestes termos, é fundamental que tenham acesso à informação, no caso aqui estudado, informação sobre o processo de capitalização de dados. Se estas informações não são de conhecimento comum, dificilmente se poderá tomar decisões com base em suas próprias vantagens. O que se percebe é que, ainda que seja feita uma análise das liberdades individuais para decisões com fins egoístas, ainda assim, no cenário de desconhecimento sobre as operações mercadológicas de dados, não se poderá dizer que os cidadãos são livres. Neste sentido surge uma incoerência sobre a lógica da imposição das tecnologias de vigilância: assume-se que somos muito melhores em termos práticos com elas do que de outra forma, mas não parece possível chegar a tal conclusões sem antes ter conhecimento amplo sobre o que elas significam e quais as suas consequências.

Mill também se preocupou com a participação das populações nos momentos de decisão nas questões públicas, que não deveriam ser feitas isoladamente da sociedade em geral. Tal participação dos cidadãos nas questões públicas seria importante não apenas para prevenir uma exagerada concentração de poder decisório em poucos, mas também para que a população aprendesse a participar da vida pública, associando-se em torno de interesses comuns e expressando-se nos meios deliberativos. Para o autor, participar dos momentos de deliberação é fundamental para promover um ensino sobre como ter uma vivência participativa (MILL, 2011; PATEMAN, 1992). Assumindo essa importância dada à participação popular, é preciso levantar uma das dificuldades que as Big Techs empregam sobre ela: a participação, a

deliberação, o próprio aprender sobre as questões públicas, são fenômenos profundamente influenciados por atores políticos de poder, no caso aqui trabalhado, pelas próprias Big Techs.[2]

Pode-se questionar, a partir do que foi dito, que as reflexões de Mill anteriormente apresentadas sobre a desigualdade de poder entre os Estados e os cidadãos e a relevância da participação popular em torno de assuntos públicos não podem ser tidas como verdade absolutas, mesmo porque a realidade hoje é muito diferente da considerada pelo autor. De fato, até mesmo para Mill é um erro assumir que existem verdades absolutas, ou pelo menos que estas já foram alcançadas. Se alguém discorda de algo, seja a sua discordância embasada em verdade ou não, deve ser considerada. Com o avanço dos aparelhos eletrônicos como mecanismos responsáveis por tarefas em vários momentos em nossa vida (como, por exemplo, expandir as possibilidades e a agilidade na comunicação), eles se colocam cada vez mais como verdades absolutas dos quais não se pode se livrar, em outras palavras, parece cada vez mais impossível pensar em dinâmicas sociais que desconsiderem as tecnologias de vigilância. As tecnologias, em si, não são um problema, e sim a sua razão de ser, que não é, como pode se pensar, simplesmente prover serviços e qualidade de vida para os que as detém. Pode se dizer que existe uma certa resistência a refletir criticamente sobre as consequências tecnológicas nas sociedades humanas, visto que estão estreitamente relacionadas à noção de progresso e conhecimento, de forma que dificilmente poderia significar mal às pessoas. Assume-se como uma verdade mais ou menos incontestável que tais tecnologias nos fizeram bem, e apenas isto importa. Como Mill propriamente coloca, existe uma grande diferença entre considerar um pensamento como verdade após este ser confrontado com o contraditório, e entre assumir como uma verdade indiscutível para impedir refutação.

No que diz respeito à regulação das liberdades empresariais, Mill, que defende abertamente a ideia de livre regulação do mercado, não deixa de acrescentar a importância do papel do Estado na regulação das relações de troca, para coibir, por exemplo, o mercado ilegal de venenos, pois estes podem ser usados pelos seus compradores para cometer crimes:

> Se nunca se trouxessem ou usassem venenos para propósitos outros que o de assassinar, justificar-se-ia proibir a sua fabricação e venda. Eles podem, contudo, ser necessários não só para fins inocentes, como também para fins úteis, e não é possível impor restrições num caso sem operarem no outro. De outro lado, é função própria da autoridade pública a prevenção de acidentes. Se alguém foi visto, por um agente da autoridade ou outra qualquer pessoa, tentando atravessar uma ponte verificada perigosa, e não havia tempo de adverti-lo do perigo, essas pessoas podiam agarrá-lo e

[2] A disparidade de poder para alterar a opinião pública não é uma questão que surge no século XXI, nem mesmo com as Big Techs, no entanto, o que se enuncia aqui é o fato das Big Techs usufruírem de um expressivo poder na modulação dos processos decisórios.

> trazê-lo para trás sem lhe infringir realmente a liberdade: pois a liberdade consiste em fazer o que se deseja, e ele não deseja cair no rio (MILL, 2011, p.169)

O autor busca, neste caso, conciliar os limites da liberdade de um comprador em adquirir veneno, e a legítima função do Estado em prevenir atos criminosos que poderiam derivar desta compra. Mill percebe que a venda e a compra do veneno em si não deveriam ser de todo proibida, mas sim regulada através de um rigoroso contrato que afastasse a possibilidade do uso ilegal do próprio veneno:

> O vendedor, por exemplo, poderia ser solicitado a lançar num registro a época exata da transação, o nome e o endereço do comprador, a precisa qualidade e quantidade vendida; a perguntar o fim para que o artigo é necessitado, e registrar a resposta recebida. Quando não houvesse prescrição médica, a presença de alguma terceira pessoa poderia ser exigida, para recordar o fato ao comprador, no caso de mais tarde haver razão para acreditar ter sido o artigo aplicado a propósitos criminosos. Tal regulamentação não seria, em regra, impedimento material a obter o artigo, mas um obstáculo muito considerável a se fazer dele um uso impróprio que não fosse descoberto (MILL, 2011, p.170 e 171)

Fazendo um paralelo com o mercado de dados, os riscos postos nele também não são de todo conhecidos: quais dados são colhidos? Qual o destino deles? Serão eles vendidos? Para quem? Uma das perguntas para qual essa pesquisa mais se volta: como esse mercado atinge as pessoas sobre as quais tais dados dizem respeito? São todas perguntas de difícil resposta, e que tal dificuldade não resulta em uma redução da aquisição de dados, pelo contrário, os usuários aceitam muito bem não terem essas dúvidas respondidas (ZUBOFF, 2021). É importante perceber também que, no caso do mercado de veneno do qual trata Mill, a solução que o autor propõe a partir de um contrato rigoroso diz respeito justamente a colocar de forma mais explicita as intenções de cada parte do acordo, prevenindo assim que alguém possa ser uma ameaça estando de posse do veneno, é válido questionar se, no caso do mercado de dados, todas as partes envolvidas estão cientes das implicações da negociação.

O autor ainda destaca que ninguém tem para si a liberdade de agir e decidir pelo outro (com exceção dos casos de pessoas dependentes), isto porque tal liberdade implicaria no cerceamento da liberdade do outro, que teria suas vontades inibidas pela terceirização de suas escolhas, para Mill: “Deve haver liberdade para se fazer aquilo de que se gosta no que é estritamente de interesse individual. Mas não deve haver liberdade para agir por outro, sob o pretexto de que os negócios do outro são os nossos próprios negócios” (MILL, 2011, p.167). Nesses termos, modular o comportamento de alguém para seu próprio interesse seria uma evidente violação ao que sofre a modulação, que, como será posto adiante, é uma prática bastante intrínseca ao próprio mercado global de dados. Se os Estados violam as liberdades dos indivíduos, estarão fazendo uso abusivo de seu puder, e, uma vez que se entenda que se

submeter a esses abusos não é mais necessário e que é possível e necessário despojar os soberanos abusivos de seu poder, assim as pessoas poderão fazer.

Como ficou evidente, mesmo Stuart Mill, que é um importante autor defensor das liberdades individuais e do mercado como espaço de amplitude de tais liberdades, estabelece nítidos limites para ela, os quais podem não estar sendo respeitados nesta nova forma de mercado que se estabelece no plano transnacional. Mas Mill não foi o único autor preocupado com os limites das liberdades. John Locke (1632-1704), por exemplo, autor que inspirou a teoria de Stuart Mill, conhecido como o "pai do liberalismo", foi um importante filósofo na busca por entender a relevância do papel do Estado na sociedade, que é o de defender o que ele entendeu por direitos naturais, isto é, os direitos à vida, liberdade e propriedade. Aquele que desrespeita os direitos naturais está sob prerrogativa de punição, pois terá praticado ato violento injusto, e o responsável pela punição justa são os governos, pois estes têm legitimidade para reparar as vítimas das violências alheias. Se um governo se recusa a assumir seu dever de defender os direitos naturais, este também é injusto, e não poderá ser julgado legítimo (LOCKE, 2020). A propriedade, um dos direitos naturais para o autor, é conquistada a partir do trabalho, que é a forma legítima pela qual o ser humano pode tomar posse de algo que está na natureza. Toda a discussão referente à aquisição de propriedade feita por Locke trata da relação do homem com a natureza, isto é, apenas é possível adquirir uma propriedade no momento em que, através do trabalho, parte do que é da natureza torna-se seu legitimamente. Não há então a possibilidade de posse sobre aquilo que é parte constitutiva do outro, em nossa discussão, os dados sobre a vida privada de cada indivíduo.

Locke acredita que seja responsabilidade dos governos se sustentarem como protetores dos direitos das pessoas pois são eles que estabelecem as leis a serem seguidas. Os direitos naturais, que existem de forma independente de qualquer Estado, deverão ser respeitados a partir das leis. Como define o autor:

> A liberdade consiste em não se estar sujeito à restrição e à violência por parte de outras pessoas; o que não pode ocorrer onde não há lei: e não é, como nos foi dito, uma liberdade para todo homem agir como lhe apraz. (Quem poderia ser livre se outras pessoas pudessem lhe impor seus caprichos?) Ela se define como a liberdade, para cada um, de dispor e ordenar sobre sua própria pessoa, ações, possessões e tudo aquilo que lhe pertence, dentro da permissão das leis às quais está submetida, e, por isso, não estar sujeito à vontade arbitrária de outra pessoa, mas seguir livremente a sua própria vontade. (LOCKE, 2020, p.115.).

Cabe, portanto, questionar se os governos estão sendo eficientes na manutenção dos direitos dos cidadãos sobre os quais tem responsabilidade, no caso específico desta pesquisa, se a proposta do governo brasileiro para proteção dos direitos dos cidadãos é suficiente para os

proteger de quaisquer agressões que possam partir das Big Techs. Para isso, é preciso entender como as Big Techs e o mercado global de dados operam.

Para o desenvolvimento da pesquisa pretende-se apresentar os conceitos "capitalismo de vigilância" em profundidade, além de "Big Techs" e outros conceitos fundamentais à discussão teórica na qual esta pesquisa se encontra. A partir de uma compreensão sobre o fenômeno do capitalismo de vigilância e das suas consequências políticas, sociais e econômicas pretende-se expor de forma minuciosa a lei 13.709/2018, apresentando brevemente seu histórico formativo e o contexto político no qual foi aprovada, assim como pontos fundamentais para compreensão da questão do acúmulo de dados. Em um terceiro momento da pesquisa se apresentará uma discussão sobre qual é a função exercida por esta lei na questão envolvendo o acúmulo de dados, problema já trabalhado por alguns autores, para que, por fim, se possa elaborar uma conclusão sobre quais são os limites que a lei impõe em relação ao capitalismo de vigilância e em quais sentidos ela interage com este fenômeno. Para a efetivação da análise documental que envolve esta pesquisa, se evidenciará a relação dos artigos da lei com as características que estabelecem o capitalismo de vigilância, de forma a possibilitar uma análise relacional entre os dois principais objetos desta pesquisa.

A pesquisa pretende não desconsiderar o desequilíbrio de poder estabelecido entre os agentes, mas assumi-lo para então compreendê-lo minuciosamente. Os estudos pós-coloniais são muito úteis para este objetivo, visto que apresentam uma perspectiva de estudo que assume as hierarquizações simbólicas de dominação, especialmente nas relações de colonialidade, e buscam desconstruir símbolos totalizantes úteis à hierarquia posta entre países "centrais" em relação aos demais (COSTA,2006).

Esta pesquisa busca abranger uma perspectiva que considere as relações de colonialidade do século XXI e as desigualdades históricas desenvolvidas entre o norte e o sul global, em especial entre a Europa e os Estados Unidos em relação as demais partes do mundo. Uma série de autores buscaram superar em alguma medida a condição colonial posta no próprio desenvolvimento das ciências sociais, fazendo surgir, inclusive, estudos chamados pós-coloniais e outros decoloniais, os quais, de forma ampla, propunham estabelecer um questionamento sobre a centralidade da Europa nas questões sociais, além de trazer foco as perspectivas dos países do sul, como os que integram a América Latina e o continente africano. Esta descentralização da Europa nas ciências sociais se deu de diversas formas. Nesta pesquisa em específico, busca-se problematizar as relações de colonialidade estabelecidas dentro do sistema capitalista global de dados no século XXI a partir das desigualdades evidenciadas entre

o norte e o sul global, especialmente entre os Estados Unidos e demais países[3]. A importância que se dá ao desequilíbrio de poder existe porque:

> Pensar o capitalismo sem a colonialidade é observar unilateralmente o problema e sua solução, considerando apenas o olhar de quem está no centro do sistema mundo. Pensar o capitalismo com a colonialidade significa diversificar o olhar crítico para contemplar a diversidade de situações particulares a partir das quais se vive o capitalismo colonial e sua contestação (MARTINS, 2017, p.47.).

Desta forma, considerar a colonialidade ao se estudar um momento do capitalismo, no caso, o capitalismo de vigilância, é fundamental para que se estabeleça uma leitura mais abrangente sobre as partes envolvidas nas relações transnacionais, pois, como o capitalismo de vigilância envolve muitos países e as relações de poder entre eles, uma leitura mais abrangente se faz necessária.

Por fim, é importante destacar que as metodologias de pesquisas na área das ciências sociais aplicadas ao digital têm se desenvolvido recentemente, por vezes voltando-se aos clássicos e por vezes se inovando aos novos desafios levantados pelos novos objetos de estudo (MISKOLCI, 2016). Por estes motivos se busca assumir uma semelhança metodológica com autores consolidados na área das ciências humanas e que se preocuparam com o estudo do meio digital de diversas formas, como Silveira (2017, 2019, 2021), Zuboff (2021) e Morozov (2018), para que, a partir destes e outros autores, seja possível construir um estudo crítico e orientado cientificamente sobre o objeto em questão, em que isso significa:

> Considerarmos criticamente o entusiasmo em relação aos big data em termos de suas potencialidades e limitações. Os big data devem ser encarados – da mesma forma que outros fenômenos – a partir de um velho princípio das ciências proposto por Francis Bacon, que foi enfatizado no nascimento da sociologia por Émile Durkheim e posteriormente entoado como um mantra por Pierre Bourdieu: o combate às noções vulgares ou praenotiones (pré-noções) (NASCIMENTO, 2016, p.226).

Em outras palavras, o que se espera é que esta pesquisa contribua no entendimento sobre os desafios sociais levantados pelo desenvolvimento e dispersão das TICs no século XXI para as sociedades e seus sistemas democráticos, assumindo as relações de colonialidade persistentes no século XXI, e como o Brasil especificamente buscou lidar com tais desafios a partir da lei 13.709/2018, chamada Lei Geral de Proteção de Dados.

[3] Como ficará evidente ao longo da pesquisa, ao tratar de capitalismo de vigilância, a desigualdade geopolítica se estabelece entre os Estados Unidos e outros países do mundo.

2. Capitalismo de vigilância, Big Techs e Colonialismo de dados

A relevância que o acúmulo de dados ganhou para o cenário econômico e político mundial levou muitos pesquisadores a considera-lo o "novo petróleo" (VIANNA, 2021). Esta comparação se dá pelo fato de que os dados se tornaram um importante capital especulativo, regido majoritariamente pelas elites do norte global, as quais compartilham de um grande interesse por ele, como será mais adequadamente explorado adiante. Por mais que, em alguma medida, tal comparação seja cabível, vale ressaltar que os dados são um capital muito diverso do petróleo, ou de qualquer outro que é retirado da natureza pelo humano para ser comercializado e acumulado em razão de seus valores. O acúmulo dos dados, diferentemente do acúmulo de petróleo, exige uma extensa e frequente colaboração de uma quantidade significativa de pessoas para que tenha tão relevante significado econômico, como tem nos dias de hoje.

Shoshana Zuboff foi uma importante filósofa e psicóloga que buscou elucidar como o mercado global de dados opera, e, para isso, desenvolveu o conceito "capitalismo de vigilância". Capitalismo de vigilância se refere a "uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas" (ZUBOFF,2021, p.13). Para que seja possível submeter a experiência humana à condição de mercadoria, é necessário que tais experiências sejam, ao máximo possível, captadas e armazenadas na forma de dados, e que tais dados tenham valor de troca. É importante, ainda, aos capitalistas de vigilância, poderem realizar esta prática livre de limitações legais, nos mais variados territórios. Existe, portanto, grande interesse dos capitalistas de vigilância em não se limitar a fronteiras nacionais, a políticas de privacidade, ou mesmo a legislações no momento em que estas venham a ferir seus interesses.

Para que o capitalista possa agir livremente na coleta e capitalização de experiência, mais do que recusar medidas legais que o restrinja, é necessário colocar-se como dono do meio pelo qual os seres humanos realizam suas experiências: os meios digitais estão postos na sociedade em grandes quantidades, e garantem acessibilidade a mecanismos que permitem o pleno armazenamento de dados comportamentais. Facebook, Google, e outros sites amplamente utilizados pela população operam como sequestradores de dados para os capitalistas de vigilância, que são aqueles que capitalizam a experiência humana, ou ainda, aqueles que são capazes de, a partir da experiência humana, atingir as receitas de vigilância. As receitas de vigilância são propriamente o ganho financeiro advindo da coleta e venda de informações

pessoais dos usuários que indiquem seus comportamentos futuros: “Os verdadeiros clientes do capitalismo de vigilância são as empresas que negociam nos mercados de comportamento futuro” (ZUBOFF, 2021, p.12).

A chamada nova ordem econômica apenas pode se sustentar devido ao acúmulo em grande, e sempre maior, escala de dados comportamentais. Para tanto, os capitalistas de vigilância apresentam suas tecnologias aos cidadãos, da forma mais acessível possível, e garantem que essas ferramentas sejam capazes de “sequestrar”, como Zuboff (2021) coloca, o maior número de dados do maior número de pessoas possível. O acúmulo destes dados não tem a simples pretensão de aperfeiçoar as funções das tecnologias à população, mas sim a de colher tantos dados que seja possível predizer ações a serem realizadas pelos indivíduos, com o uso de tecnologias criadas para esse fim. A junção de tantos dados permite conhecer predileções comportamentais, isto é, como se age no meio digital e real, e como se reage a diferentes estímulos. Portanto, a predileção da ação humana está submetida à condição de produto. Estes produtos de predição podem então ser direcionados ao mercado de predições, que negocia informações sobre as ações futuras dos indivíduos, formando o que Zuboff chamou de mercado em comportamento futuro, que garantirá as empresas capitalistas de vigilância receita de vigilância, isto é, a remuneração pela vigia e pelo armazenamento massivo de dados. Alguns dados sustentam a relação entre vigilância e lucro: a empresa Alphabet, detentora da Google, teve 89% do seu lucro resultante de publicidade realizada pelo Google, o qual tem registrado em sua plataforma, em média, 1,2 trilhão de pesquisas por ano (ZUBOFF, 2021). É preciso responder o porquê de a predileção dos comportamentos possuir tanto valor de mercado e qual sua relação com a coleta de informações. Primeiramente, sabe-se que a coleta de dados não ocorre com o intuito único de ampliar a eficiência de seus produtos, mas sim com o objetivo de coletar o maior número possível de informação, de forma que seja possível estabelecer as predileções comportamentais para cada indivíduo. Uma vez que as máquinas tenham vigiado o comportamento dos indivíduos por tempo suficiente, será possível entender suas preferências, repulsas, conhecer seus:

> Gostos, sentimentos, projetos, hábitos, posições políticas, posições religiosas etc., são as informações geradas pelo homem moderno, ainda na forma de dados em estado bruto. O uso da tecnologia refina e extrai dos dados para que eles se tornem predição de comportamentos, ou seja, para atuarem na previsibilidade dos passos do usuário. Com isso, as empresas vendem a possibilidade de influência sobre os usuários, porém, muitas vezes partem de informações que o usuário não permitiu a finalidade utilizada. (CARVALHO, 2019, p.55).

É a predição comportamental que permite o superávit comportamental, isto é, o lucro que se obtém a partir da predição alcançada a partir dos dados. Nas palavras da autora:

> Em suma, o superávit comportamental sobre o qual se assenta a fortuna do Google pode ser considerado *ativos de vigilância*. Esses ativos são matérias-primas críticas na busca por *receitas de vigilância* e sua conversão em *capital de vigilância*. A lógica inteira dessa acumulação de capital é entendida com mais exatidão como *capitalismo de vigilância*, que é a estrutura fundacional para uma ordem econômica baseada na vigilância: uma *economia de vigilância*. o ponto-chave de que a essência da exploração, aqui, é a utilização de nossa vida como dados comportamentais para o aperfeiçoamento do controle de outros sobre nós. (ZUBOFF, 2021, p.145 e 146).

O Google foi a primeira empresa a perceber no acúmulo de dados do usuário um ativo econômico muito valoroso, o que motivou a empresa a cada vez mais desenvolver o imperativo de extração destes dados, possibilitando o cada vez mais expansivo lucro. Zuboff percebe que, apesar do capitalismo de vigilância depender de aparelhos tecnológicos, não foi a mera existência deles na sociedade que eclodiram na sua formação, pelo contrário, esta nova ordem econômica é produto de um setor empresarial específico estabelecido nos Estados Unidos, o qual estabeleceu novos imperativos que dominariam sobre essa forma econômica: o imperativo de extração e o de predileção. Na verdade, isso é fruto de uma elaboração bem sucedida em um momento histórico propício, e outras empresas estadunidenses se somaram à Alphabet no grupo de empresas com ativos de vigilância: Facebook, Microsoft, Apple, Amazon e Uber formaram o seleto grupo de empresas detentoras de tecnologia para captar lucro a partir de acúmulos de dados (Zuboff, 2021). A citação abaixo permite entender, em alguma medida, como opera o mercado de propaganda direcionada:

> O RTB é um modelo transformador para o mercado, baseado em eficiência de custos e que ajudou o setor a ser mais assertivo e, ao mesmo tempo, garantir que os usuários pudessem receber anúncios melhores e mais atraentes. O modelo funciona, de forma bem simplificada, a partir de uma cadeia de dois lados, da seguinte forma: (i) no "lado da oferta", um veículo (como um site ou aplicativo) disponibiliza seu inventário de espaços publicitários por meio de soluções de software conhecidas como supply-side platforms ("SSP"); (ii) essas SSPs vão enviar um pedido (conhecido como bid request), por conta e ordem do veículo, para um outro tipo de tecnologia, as ad exchanges; (iii) as ad exchanges, por sua vez, vão solicitar que compradores realizem uma oferta para aquele espaço publicitário; (iv) do outro lado da cadeia (o "lado da demanda"), possíveis compradores (anunciantes e agências de publicidade) vão enviar as suas ofertas de compra por meio de tecnologias conhecidas como demand-side platforms ("DSP"); (v) as DSPs também vão se conectar às ad exchanges, e vão analisar os bid requests enviados pelas SSPs; (vi) uma vez que todos estejam conectados nesse mesmo ambiente, as DSPs irão analisar os bid requests oferecidos pela SSPs, e apresentar uma proposta de preço (um lance) para inserir um anúncio naquele espaço publicitário (vii) a ad exchange, de maneira semelhante a um leiloeiro, irá coordenar a dinâmica entre os diferentes lances de DSPs para um determinado bid request; (viii) a DSP que oferecer o maior lance será vencedora, e as tecnologias irão trabalhar para que o anúncio vencedor seja inserido no espaço publicitário do publisher - todo esse processo dura apenas alguns milissegundos! (RAMOS, 2019, p .6 e 7)[4]

[4] RTB se refere aos mecanismos automatizados de publicidade que operam na internet.

Ainda que todo este processo pareça uma automatização de um sistema de propagandas convencional, ele não se dá sem o incremento fundamental à pesquisa que é o uso dos dados para ampliar a eficiência deste processo:

> Surgem ferramentas de tecnologia cujo objetivo principal é automatizar os processos de identificação de conteúdo nas páginas e entregar publicidade segmentada de acordo com o conteúdo identificado. Por meio de cookies, tags, gerenciadores de base de dados e outras tecnologias, essas ferramentas não buscavam redefinir o processo de negociação de publicidade, mas tão somente automatizá-lo. Surgem então tecnologias de publicidade comportamental, que permitem a identificação do histórico de navegação do usuário e o processamento dessas informações em grandes bases de dados, de forma a segmentar a entrega de publicidade especificamente para aquele usuário que atende ao perfil de determinado anunciante (RAMOS, 2019, p. 5 e 6).

Tendo compreendido a problemática a ser tratada, se avança para a análise de certas consequências sociais e políticas dela.

2.1 Sociedade disciplinar e sociedade de controle

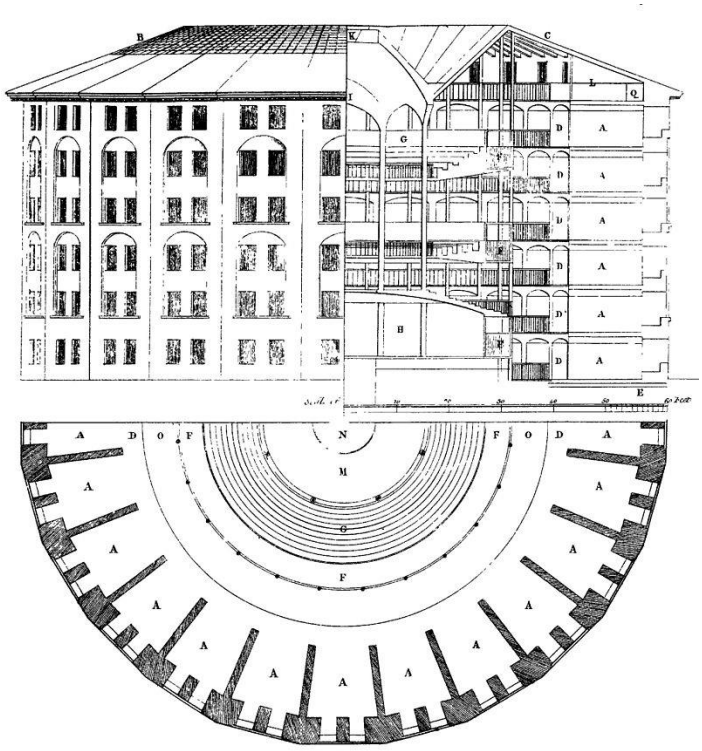
A discussão sobre vigilância não nasce junto do capitalismo de vigilância. Na verdade, Foucault (1975) já analisava o sentido vigilante que se desenvolvia em diversas instituições sociais disciplinadoras, como as escolas e os presídios. Para o autor, não haveria necessidade de uma constante punição sobre os cidadãos para fazerem se comportar da forma que se desejasse, muito embora, como ele mesmo demonstra, por muito tempo este tenha sido o método utilizado. A vigilância constante de um sujeito, punindo-o apenas quando este se comporta de forma não desejada, fará com que a própria vigilância seja capaz de estabelecer o comportamento desejado, mais do que isso, o sentimento de ser vigiado, por si, opera sobre os sujeitos como um mecanismo de poder que apara os comportamentos indesejados pelo que tem o poder de punir, mesmo que este não exerça nenhuma força física sobre o vigiado, o que faz descartável a própria vigilância constante, considerar-se vigiado já faz exercer o controle. O exercício do poder em prol da disciplina se dá através dos dispositivos disciplinadores, sendo esses dispositivos entendidos como mecanismos sociais capazes de gerar coesão ao estabelecer um padrão normativo, como a escola, a família e os presídios: “Um dispositivo também pode ser conceitualizado como uma configuração específica de domínios do saber e de modalidades de exercício do poder, a qual possui uma função estratégica, em relação a problemas considerados cruciais em um momento histórico” (WEIMANN, 2006, p.17).

Para exemplificar uma sociedade disciplinar, Foucault volta-se ao modelo do panóptico, isto é, uma estrutura elaborada por Jeremy Bentham, um importante filósofo inglês, no fim do século XVIII, e que tinha por pretensão ser um modelo de penitenciaria eficiente para sua época:

> O edifício é circular. Os apartamentos dos prisioneiros ocupam a circunferência. Você pode chama-los, se quiser, de celas. Essas celas são separadas entre si e os prisioneiros, dessa forma, impedidos de qualquer comunicação entre eles, por partições, na forma de raios que saem da circunferência em direção ao centro, estendendo-se por tantos pés quantos forem necessários para se obter uma cela maior. O apartamento do inspetor ocupa o centro; você pode chama-lo, se quiser, de alojamento do inspetor. Será conveniente, na maioria dos casos, se não em todos, ter-se uma área ou um espaço vazio em toda volta, entre esse centro e essa circunferência. Você pode chama-lo, se quiser, de área intermediária ou anular. Cerca do equivalente da largura de uma cela será suficiente para uma passagem que vai do exterior do edifício ao alojamento. Cada cela tem, na circunferência que dá para o exterior, uma janela, suficientemente larga não apenas para iluminar a cela, mas para, através dela, permitir luz suficiente para a parte correspondente do alojamento. A circunferência interior da cela é formada por uma grade de ferro suficientemente fina para não subtrair qualquer parte da cela da visão do inspetor (BENTHAM, 2019, p.20 e 21)

Assim, no panóptico de Jeremy Bentham, todos os presentes são postos de forma isolada em partes do edifício circular na qual há luz que ilumine suas localidades. Em uma posição privilegiada se encontra o vigia, que, ainda que seja uma só pessoa, será capaz de observar todos os espaços da torre ocupados, de forma que não possa ser visto pelos vigiados. Esta estrutura gera um expressivo poder ao vigilante em relação aos vigiados: enquanto um observador detém o poder ao ter pleno conhecimento sobre tudo que os demais fazem, os demais se quer sabem se estão sendo vigiados ou não (BENTHAM, 2019; FOUCALT, 1979). Como se pode perceber, o panóptico pode ser um modelo de estrutura penitenciária eficiente, pois permite um amplo poder de vigília ao inspetor, e, portanto, sobre os que estivessem em seu interior. Este modelo emula uma sociedade disciplinar, isto é, uma sociedade regrada por diversos dispositivos disciplinadores que operam em espaços bem definidos e com hierarquia inviolável (COSTA, 2004).

Figura 1- Panóptico de Bentham, desenho de Willey Revelley, 1791



Fonte: CARVALHO NUNES, 2020 apud Wikimedia Commons

A figura acima ilustra a arquitetura de uma unidade prisional inspira no modelo de Bentham.

Foucault percebeu ainda que o poder de vigilância para disciplina sobre os cidadãos também carregue as suas particularidades em relação ao panóptico. Diferentemente do panóptico de Bentham, em que um número reduzido de indivíduos pode ser totalmente observado por um único vigia ou poucos vigias, os governos precisam estabelecer vigilância sobre um número muito maior de pessoas para estabelecer disciplina, se possível, a todas elas, garantindo ainda punição, ou o medo dela, a todas aqueles que se voltarem contra o padrão normativo. Para tanto, são elaboradas as biopolíticas: um conjunto de ações capazes de fazer com que o Estado tenha conhecimento da vida dos cidadãos (através de dados estatísticos, quantificações e comparações com outros grupos populacionais) e, a partir deste conhecimento, estabeleça a disciplina sobre seus corpos, sigam uma rotina bem estabelecida e assumam uma padronização de seus comportamentos. As biopolíticas podem servir a diversas funções a partir da vigilância, sendo que o Estado pode usar delas para colaborar com as estruturas de mercado, sustentando, assim, uma relação cooperativa entre Estado e mercado (BARROS, 2020).

Com o desenvolvimento da tecnologia e sua maior presença na vida dos cidadãos, novos mecanismos de vigilância e controle se estabeleceram, estes foram chamados de dispositivos tecnopolíticos:

> denomino como dispositivos tecnopolíticos o conjunto de técnicas de vigilância e controle, relacionadas às TICs (Tecnologias de Informação e Comunicação) – abrangendo conglomerados empresariais de tecnologia, sistemas de inteligência estatais, plataformas digitais, gadgets, softwares e aplicativos presentes no cotidiano das pessoas –que se baseiam na coleta, processamento, análise e utilização de uma quantidade massiva de dados para gerenciamento e regulação das vidas humanas (BARROS, 2020, p.7).

Assim como os dispositivos antes apresentados buscam estabelecer disciplina a partir da vigilância, os dispositivos tecnopolíticos se utilizam da necessária e constante relação do sujeito com os aparelhos tecnológicos para exacerbar a vigilância e ter, consequentemente, maior poder disciplinador sobre os usuários, seja de forma individual, como os dispositivos disciplinadores, seja através de biopolítica (BARROS, 2020).

A tecnopolítica pode se favorecer e muito dos algoritmos, coisa que os dispositivos disciplinadores do século XX não podiam. No século passado, quase todo o processo envolvendo vigiar e punir deveria ocorrer a partir de humanos, que são consideravelmente mais limitados que os algoritmos ao se tratar de captura, armazenamento e interconexão de dados, no desenvolver da modernidade é que as formas de controle pela vigilância se alteram:

> A sociedade pós-moderna é caracterizada, essencialmente, por reduzir as atitudes autoritárias e dirigistas e, ao mesmo tempo, por aumentar a oportunidade das escolhas particulares, a privilegiar a diversidade. Entretanto, é preciso ressaltar que essa libertação em face das tradições e esse acesso a uma autonomia real não significaram o desaparecimento de todas as espécies de poder sobre os indivíduos. Não se pode dizer que a pós-modernidade inaugurou um mundo ideal, sem conflito e sem dominação. Ao contrário, os mecanismos de controle permanecem, mas de forma adaptada, mais sutil (BAIÃO; GONÇALVES, 2014, p.4).

Os algoritmos e as tecnologias de vigilância cada vez mais avançadas fazem com que as sociedades assumam novas formas organizacionais distintas da sociedade disciplinar. Delluze e uma série de autores a partir de seus escritos desenvolveram o conceito de sociedade de controle para se referir a essas novidades no sentido vigilante das sociedades:

> Deleuze percebe no enclausuramento a operação fundamental da sociedade disciplinar, com sua repartição do espaço em meios fechados (escolas, hospitais, indústrias, prisão...), e sua ordenação do tempo de trabalho. Ele chamou esses processos de moldagem, pois um mesmo molde fixo e definido poderia ser aplicado às mais diversas formas sociais. Já a sociedade de controle seria marcada pela interpenetração dos espaços, por sua suposta ausência de limites definidos (a rede) e pela instauração de um tempo contínuo no qual os indivíduos nunca conseguiriam terminar coisa nenhuma, pois estariam sempre enredados numa espécie de formação permanente, de dívida impagável, prisioneiros em campo aberto (COSTA, 2004, p.161)

A condição de prisioneiros em campo aberto diz muito sobre a sensação de liberdade que faz parte da sociedade de controle, e que marca uma forte distinção em relação a sociedade disciplinar. A sensação de liberdade posta na sociedade de controle advém da difusão das formas de controle sociais que, não mais restritas a espaços e tempos definidos, cercam as populações independentemente de suas localidades. A sociedade de controle é resultado do avanço dos mecanismos de controle sobre as populações, que passam a ser identificadas independentemente da forma com a qual vivam, pois, independentemente de suas escolhas, são identificados e vigiados. Neste sentido pode se dizer sobre o sentido social dado às tecnologias, e como os algoritmos e todos os mecanismos que os envolvem atingem diretamente as sociedades.

> Portanto, sob a perspectiva da sociedade de controle, sistemas algorítmicos seriam tecnologias antes sociais do que técnicas, dispositivos das técnicas de poder e controle contemporâneas. Como outros dispositivos, teriam como objetivo integrar multiplicidades, criando grupos imbuídos de propósito (docilidade e cooperação frente ao capitalismo contemporâneo). (ARRUDA, 2019, p.10).

Independentemente das particularidades dos grupos e dos indivíduos que os formam, todos são submetidos a condição de vigilância e controle, e contribuem para a perpetuação da sociedade de controle e do capitalismo de vigilância a partir de seus comportamentos, sejam eles quais forem. Disto deriva um contrassenso inerente à sociedade de controle: todos sentem-se mais livres para agir e escolher, mas suas escolhas e comportamentos não significa liberdade para estar fora dos limites de controle e vigilância. Enfim, pode se assinalar que na sociedade de controle, a vigilância se tornou dispersa, uma vez que são diversas tecnologias atuando com o objetivo de vigiar; impessoal, uma vez que se vigiam inúmeras pessoas sem critérios fixos que definam quem vigiar e quem não; e horizontalizada, já que os aparelhos de vigilância estariam disseminadas entre os membros da sociedade. Se antes a vigilância se dava em espaços definidos, como escolas, hospitais e penitenciárias, e por um tempo também definido, agora ela ocorre por tempo indeterminado e em espaços indefinidos (COSTA, 2004).

É importante constatar que, embora tanto Foucault quanto Zuboff estejam tratando de vigilância, não tratam da mesma forma nem da mesma dimensão, visto a distância temporal entre os estudos dos autores e seus objetivos. Zuboff não buscou atualizar o pensamento de Foucault, ou atingir novas conclusões a partir de seus conceitos, mas sim pensar a vigilância como parte fundamental de uma nova dimensão capitalista. Quando Vigiar e Punir foi publicado originalmente, em 1975, a vigilância foi analisada como tendo por fim a disciplina, isto é, a vigilância foi entendida como um mecanismo pela garantia de comportamentos e exercício de poder. Enquanto a vigilância tratada por Foucault como diretamente vinculada a uma possível

punição, pouco há de se dizer sobre punição na vigilância tratada por Zuboff, já que o comportamento desejado é o não censurado, a exposição que mais expressa os desejos dos usuários. O único comportamento passível de punição é a não submissão a vigília, porém, como se evidenciará ao decorrer da pesquisa, o indivíduo não possui liberdade para tanto.

Isto não significa que a vigilância para a adestramento dos comportamentos inexiste no capitalismo de vigilância, pelo contrário, ainda assim há a modulação dos comportamentos dos usuários através dos mecanismos presentes na própria rede, intituladas tecnopolíticas. Alguns destes mecanismos de controle são: o pastoreio, que se entende pela prática de limitação de possibilidades do usuário para que esse possa apenas tomar as decisões desejadas pelas empresas; o *turning*, que se refere aos sinais postos para provocar uma tendência comportamental, como propagandas apresentadas no momento mais conveniente para a compra, e, por fim, o condicionamento, que se dá com o sistema de recompensas (quando o usuário é um bom consumidor) (ARRUDA, 2019). Percebe-se que os mecanismos de controle estão todos voltados para a sustentação do ser consumidor, que, desconhecendo a situação de controle posta sobre ele, não irá então criticá-la e poderá sentir-se livre em suas decisões.

A vigilância, sem limites bem definidos, se desenvolve junto às cidades que comportam diversos mecanismos de vigilância nos espaços públicos. Por mais que a vigilância se dê, em larga medida, no espaço virtual, ela é “uma prática marcadamente espacial” (MELGAÇO, P.1, 2015), ou seja, no espaço físico também são deixadas informações sobre os que circulam nele, e quanto mais informatizada for a cidade, mais desses dados poderão ser captados. Estas cidades são muitas vezes chamadas *smartcities* ou cidades 2.0 (MELGAÇO, 2015). Ainda que se tenha em evidência o caráter vigilante dessas cidades, afastar-se delas não significa, na prática, ter fugido da condição de vigiado. Como foi posto anteriormente, a vigilância ocorre mesmo que não se esteja em um local público, o que mostra mais uma dificuldade dos cidadãos ao tentar limitar a circulação de seus dados: limitar certos locais em detrimento de outros não é uma ação efetiva para proteger-se, nem mesmo limitar a própria exposição fará com que a coleta de dados sobre o usuário seja menos eficiente, fica, então, cada vez mais evidente o descontrole dos indivíduos sobre o que será ou não acessível pelas tecnologias.

Como se afirmou anteriormente, a presença das tecnologias responsáveis por possibilitar captura de dados é cada vez mais presente na vida dos cidadãos. Algumas já estão bem consolidadas, como os celulares e computadores, porém muitas mais tecnologias são desenvolvidas com este intuito. Em 2021 a antiga empresa *facebook* foi renomeada enquanto *meta*, e apresentou seu plano para o futuro enquanto empresa. Nas palavras de Mark

Zuckerberg, criador do *facebook: "*the next platform and medium will be even more immersive (do que notebooks e celulares) and embodied internet where you're in the experience, not just looking at it. And we call this the metaverse. You'll be able to do almost anything you can imagine" (ZUKEMBERG, 2021). O metaverso seria uma plataforma capaz de recriar espaços reais digitalmente, além de criar espaços inexistentes na realidade, para que então as pessoas possam ter um convívio altamente imersivo nesta dimensão virtual. O metaverso não se pretende meramente uma plataforma para entretenimento, mas também para reuniões e trabalho. O metaverso, se bem sucedido, significaria a plena imersão dos cidadãos no espaço virtual gerido pelas máquinas, que, estabelecendo-se enquanto espaço necessariamente acessado, levaria a uma plena dependência dos humanos sobre as máquinas para a sua relação com o espaço, agora totalmente digital.

Esta relação de dependência se sustenta também pela evidente impotência de intervenção do sujeito sobre o mundo, pois este mundo virtual não é sequer administrado pelo humano pois, ainda que seja feito para ele, o seu controle se mantém preservado pelas máquinas, cujo funcionamento é conhecido por poucos. Trata-se, desta forma, de uma condição alienada do consumidor sobre o espaço virtual consumido: não se conhece seu processo de produção, apenas se consome o produto e se torna dependente dele. É possível que não se conheça nem mesmo todas as trocas que se realizam ao acessar esta dimensão virtual, o que, como antes exposto, já acontece, se tratando da vigilância nas redes. Além deste evidente problema, o poder de vigilância é expandido consideravelmente: se antes ele ainda dependia de celulares, câmeras, computadores, e demais aparelhos, com a pessoa totalmente imersa no meio digital, todo o seu comportamento é passível de ser armazenado, mais do que isso, tratando-se de um espaço totalmente virtual, as ações que podem ou não ser tomadas também são delimitadas, ou seja, todo o comportamento se dará em favor da tecnologia que cerca o humano.

Assim, ainda que o metaverso, atualmente, seja apenas um plano empresarial, não deixa de ser importante para a pesquisa examinar os rumos que uma empresa conhecidamente captadora de dados pretende tomar. Ampliar as funções dos aparelhos, expandir as relações de dependência e o poder de vigilância, são exacerbações do que já está sendo apontado como um problema por Zuboff, Arruda e tantos outros.

2.2 Os novos imperativos do capitalismo de vigilância

Essa nova ordem econômica se sustenta a partir dos novos imperativos que pautarão as relações comerciais, os processos e a significação dos objetos fundamentais à esta nova ordem.

Como foi dito anteriormente, o capitalismo de vigilância é pautado pela comercialização de dados, o que significa dizer que, talvez, nunca anteriormente tenha havido maior relação entre informação e lucro: quanto mais informações são acumuladas pelas empresas de tecnologia, mais lucro é garantido por elas. Esses dados precisam ser retirados de seu estado bruto e trabalhados para que possam efetivamente ser utilizados mercadologicamente, o que torna necessária a sua constante e sempre maior extração: os comportamentos precisam ser tidos como dados, e os dados devem ser extraídos do âmbito pessoal e torna-lo de posse de outra pessoa, no caso, de posse das grandes empresas de tecnologia. Nesse sentido, o primeiro imperativo, o imperativo de extração, se faz fundamental para que se possa iniciar a formação desta estrutura econômica que sustenta o capitalismo de vigilância: sem a extração dos dados não há capitalização deles, e a própria razão de ser das máquinas deixaria de ser o de vigilância, bem como a função dos algoritmos. Como coloca Zuboff: "Exigir privacidade dos capitalistas de vigilância ou pressionar pelo fim da vigilância comercial na internet é como pedir a Henry Ford que faça cada Modelo T a mão ou pedir a uma girafa que encurte o pescoço. Tais exigências são ameaças existenciais" (ZUBOFF, 2021, p.291). A extração e posse destes dados por grandes empresas não se convertem em lucro se não oferecem nenhum potencial mercadológico, e o potencial que oferecem é justamente o de predileção. A soma indefinível de dados posta sob operação de algoritmos é capaz de estabelecer, em considerável medida, quais comportamentos serão mais prováveis, quais categorias de mercadoria estão mais propício a venda, por quais preços, enfim, as tendências do consumo passam não apenas a serem conhecidas como a serem moduladas, o que dá forma ao imperativo de predileção.

A modulação de comportamento se dá de várias formas, sendo sutil ou não:

> elas incentivam, sintonizam, vigiam, manipulam e modificam o comportamento em direções específicas ao executar ações sutis, tais como inserir uma frase específica no feed de notícias do Facebook, programar o surgimento de um botão "COMPRAR" na tela do seu celular, ou desligar o motor do seu carro quando um pagamento do seguro está atrasado" (ZUBOFF, 2021, p.303).

Estes imperativos assinalam uma inversão no que intuitivamente poderia se supor: não são os usuários que têm posse e controle sob a operação das máquinas, mas sim o inverso: a extração e predileção da experiência humana assinala a posse dos algoritmos (e, consequentemente, daqueles de posse deste algoritmos) sobre a experiência humana, ou, ainda: "a metamorfose da infraestrutura digital de uma coisa que temos para uma coisa que nos tem" (ZUBOFF, 2021, p.306). Na relação entre cidadão e máquinas de vigilância, um possui ao outro: o cidadão, enquanto consumidor, por meio da compra, fez daquela máquina sua, e a

máquina, a partir da modulação comportamental, possui em certa proporção o cidadão, não o possui para si, mas para a empresa que a detêm.

2.3 Divisão da aprendizagem

Pode se questionar o porquê destas poucas empresas deterem o conhecimento para ocupar uma posição tão privilegiada nesta ordem econômica, ou, ainda, por que tão poucas empresas são consideradas capitalistas de vigilância. A divisão desigual da aprendizagem é parte fundamental da sustentação do capitalismo de vigilância. Apesar dessa grande relevância e de serem bastante considerados dentro das pesquisas sobre o capitalismo de vigilância, a forma com a qual operam tecnicamente é pouco difundida, e esta é uma das grandes dificuldades de estudar os algoritmos: há uma obscuridade posta sobre o seu funcionamento:

> de várias formas, os algoritmos continuam fora do nosso alcance e eles são projetados para continuar mesmo. Isso não quer dizer que não devemos aspirar a iluminar seu funcionamento e a seu impacto. Nós deveríamos. Mas talvez nós também precisemos nos preparar para nos depararmos, mais e mais, com associações inesperadas e indescritíveis que eles vão desenhar para nós, às vezes; a incerteza fundamental sobre com quem estamos falando ou quem estamos ouvindo; e as implicações palpáveis, porém opacas, que se movem silenciosamente por baixo do conhecimento quando ele é gerenciado por algoritmos (GILLESPIE, 2018, p.117 a 118).

Poucas pessoas têm o conhecimento sobre como operam os aparelhos de vigilância, que são atualizados com grande rapidez, e ainda menos têm acesso ao modo operacional algorítmico destas máquinas. Esse grupo de trabalhadores com conhecimento suficiente para trabalhar e moldar algoritmos e máquinas de vigilância estão a serviço dessas grandes empresas não para outra coisa que não aumentar a sua capacidade produtiva, isto é, aumentar a capacidade rentável do mercado de dados, é o mercado de dados que decide quais funcionalidade serão dadas as máquinas; a internet, que já foi vislumbrada como grande potência para a consagração da democracia em um patamar não antes visto, está posta como instrumento rentável de grandes corporações estrangeiras, um objeto de disputa entre capitalistas de vigilância em busca de preestabelecer comportamentos, desejos e consumos. Zuboff conclui: “Da forma como as coisas estão hoje, são as corporações capitalistas de vigilância que *conhecem*. É a forma de mercado que *decide*. É a luta competitiva entre os capitalistas de vigilância que decide quem decide*”* (ZUBOFF, 2021, P.292).

2.4 Modulação comportamental/ algoritmos

Ao conhecer o perfil do usuário em profundidade, é possível estipular quais serão suas ações futuras, o que desejará consumir e em quais momentos. Para favorecer a realização das ações que se deseja, os usuários são submetidos ao controle das propagandas que ocorrem na

escolha do que o usuário irá ver e em qual momento, sendo as propagandas estimulantes para a realização desejada pelos empresários afim de vender seus produtos (ZUBOFF, 2021). Sendo assim, poder conhecer as futuras ações dos indivíduos possui grande valor de mercado, uma vez que se podem ofertar determinados produtos nos momentos em que os agentes estejam mais propícios a de fato compra-los, afetando positivamente os lucros dos vendedores. Isso só é possível graças a eficiência dos algoritmos em modular os comportamentos dos usuários. Os algoritmos são instrumentos tecnológicos capazes de instruir máquinas para que essas assumam uma forma lógica de comportamento diante de um ou mais problemas, que pode variar de acordo com sua programação, nas palavras de Silveira (2019):

> Algoritmo é um método para solucionar um problema. Dependente das instruções inequívocas, das regras logicamente encadeadas e de informações iniciais. Algoritmos tratam os dados de entrada que serão processados conforme os procedimentos definidos e geram resultados expressos em outros dados ou informações (SILVEIRA, 2019, p. 6).

Ao se tratar dos algoritmos com capacidade de "aprendizado" (as com tecnologia machine learning) esse comportamento algoritmo se torna muito mais complexo, pois suas conclusões são moldáveis a partir de uma série de fatores decididos no momento da programação, de forma que nem mesmo os desenvolvedores seriam capazes de prever com exatidão as ações desses algoritmos a longo prazo. Como exemplo que sustente essa conclusão, Silveira apresenta o dado de que, nos Estados Unidos, uma série de Estados usam algoritmos como ferramenta para definição de penas por crimes, e, uma das consequências foi uma extensão do racismo judiciário: os algoritmos assumiam conclusões discrepantes a partir de elementos raciais (SILVEIRA, 2019; SILVEIRA, 2017). Através do algoritmo é possível estabelecer como uma máquina irá se comportar diante de um determinado dado, e esta automatização da relação entre dado e ação das máquinas é o que permite a modulação comportamental das pessoas, isto porquê ela permite que as ações dos usuários, ao serem convertidas em dados e submetidos a análise das máquina, gerem a reação que os programadores das máquinas estabeleceram como correta e, assim, controlar a experiência de qualquer usuário ao controlar com o que estes terão contato.

A pesquisadora Debora Franco Machado elaborou uma pesquisa com o objetivo de dimensionar o que exatamente pode ser usado enquanto dado para operação de algoritmos, para tanto, voltou-se às patentes da empresa Facebook para analisar quais delas estavam direcionadas à operação moduladora. Algumas das patentes que a autora apresenta são:

> Segundo o texto da patente intitulada Pushing news feed content to client devices, para que as publicações do Feed de Notícias sejam as mais recentes possíveis no

> momento em que o usuário abre o aplicativo, é necessário calcular o horário exato em que o Feed de Notícias deve ser atualizado e qual o melhor conteúdo para ser apresentado naquele exato momento. Para isso, o sistema identifica dados do usuário, como o seu padrão de uso da plataforma e a qualidade da conexão e da memória do dispositivo. (MACHADO, P.102)

A pesquisadora ainda identificou o grande interesse da empresa em poder dimensionar os sentimentos de seus usuários enquanto utilizam seus serviços:

> Durante a pesquisa foi possível identificar interesse por parte da empresa em desenvolver e patentear sistemas capazes de coletar e inferir emoções e sentimentos dos usuários, e em usá-los como informações relevantes para a personalização, a recomendação e o ranqueamento de conteúdo. Das 41 patentes selecionadas como úteis à modulação de comportamento, seis citam a análise de sentimentos ou emoções como parte de seu funcionamento. Um sentimento específico, o tédio, é o foco da patente Presenting additional content items to a social networking system user based on receiving an indication of boredom. O sistema utiliza sensores como a câmera frontal para rastrear a posição do olhar de uma pessoa e, cruzando com outros dados, identificar se o usuário está interessado no conteúdo que está vendo no momento ou não. (MACHADO, P.107)

É a partir das respostas dos usuários aos estímulos aos quais são submetidos que os algoritmos são capazes de definir o que cada indivíduo está disposto a consumir e em que momento, possibilitando uma postagem publicitária precisa e muito eficiente, tendo todo o usuário como um potencial cliente de algum produto. Com isto posto, é possível definir a modulação algorítmica como: “uma forma de controle e orientação de comportamento possibilitada por processos algorítmicos, que opera a partir da coleta massiva de dados para direcionar condutas, a atenção ou o comportamento de pessoas ou perfis” (MACHADO, 2020, p.100).

Embora os algoritmos voltem-se para uma elaboração cada vez mais complexa do perfil de cada usuário, não deixam de serem perpetuadores de comportamentos e pensamentos regressos, pois os dados os quais utilizam para estabelecer um perfil de usuário são sempre em razão dos últimos dados de que teve acesso, mas, considerando que as pessoas podem sempre mudar suas opiniões e desejos, estes dados estão necessariamente desatualizados em relação a versão mais recente de cada pessoa:

> Esses perfis digitais, embora possam realçar a singularidade do "eu", também podem restringir a evolução e a transformação do "eu". Cada interação online é registrada e usada para refinar ainda mais o perfil do usuário, criando uma imagem estática e limitada do "eu". Isso pode restringir nossa capacidade de explorar novas identidades e de se transformar ao longo do tempo, pois somos constantemente confrontados com um reflexo digital de nós mesmos baseado em nossas ações passadas. Nesse sentido, a vigilância automatizada do capitalismo digital pode erodir a continuidade do "eu",

> enraizando-nos em uma versão codificada e potencialmente desatualizada de nós mesmos (SILVA, 2023, p.79).

Por esta razão, pode se dizer que existe nestas ações algorítmicas um tipo de paradoxo: por mais que sejam programados a construir os perfis mais detalhados de cada pessoa, condicionam as pessoas a serem o que foram antes, com os gostos e opiniões do passado, pois é sempre com o dado do passado que os dados operam. Pode-se dizer que, de certa forma, os algoritmos impõem ao usuário um modo de ser do passado.

2.5 Contratos e incontratos

O amparo legal destas empresas acumuladoras de dados se encontra na prerrogativa de que seus usuários concordaram com os termos de uso e com o compartilhamento de seus dados para que pudessem utilizar os serviços prestados pela empresa. De fato, utilizar plataformas, como facebook, instagram, whatsapp e outras exige que os usuários concordem com os termos impostos pela empresa, mas há de se questionar até que ponto os usuários têm condições de se recusar a aceitar tais contratos, e mais, se estão realmente cientes de suas proposições no momento de aceita-los. Como foi posto anteriormente, as tecnologias de vigilância se impõem a sociedade, tornando-se uma necessidade para uma série de tarefas (ZUBOFF, 2021). Alguns autores colocam que o desenvolvimento da internet e do ambiente digital são para a sociedade o que antes foi a energia elétrica, isto é, elemento tecnológico fundamental às novas necessidades humanas, e, por isso mesmo, parte estruturante das sociedades (SIQUEIRA, . N.; CONTIN. C.; BARUFI. B.; LEHFELD. 2021).

A circulação no espaço urbano, por exemplo, pode ser muito dificultada sem a utilização de aplicativos que exigem o compartilhamento da localização em tempo real, como o Google Maps, o diálogo entre pessoas distantes, o acompanhamento de notícias recentes, a elaboração de buscas por informações determinadas, enfim, são inúmeras as tarefas facilitadas e potencializadas pelos serviços prestados pelas grandes empresas de tecnologia, recusar-se a utilizá-los significaria estar em descompasso com a velocidade do presente, isto é, haverá uma desigualdade de eficiência entre aquele que pode e aceita usar as tecnologias de vigilância e os que não. O que torna tal contrato ainda mais complexo é o fato de não ser fruto de nenhuma deliberação ou concordância entre as partes: por mais que os usuários expressem aceitar os termos, em nenhum momento puderam verdadeiramente discordar do que estava posto, pois quem dita as regras do funcionamento destas tecnologias são os seus detentores. Em outras palavras, o aceite do contrato apenas formaliza as imposições das empresas de vigilância. Por este motivo Zuboff considera o "contrato" entre usuários e Big Techs como "incontratos": "o

incontrato não é um espaço de relações contratuais, mas a execução unilateral que torna essas relações desnecessárias.

Como afirma Zuboff (2021), “o incontrato dessocializa o contrato ao fabricar certeza mediante a substituição de promessas, diálogo, significado compartilhado, solução de problemas, resolução de disputas e confiança por procedimentos automatizados” (ZUBOFF, 2021, p.331). Em outras palavras, o contrato, neste caso, nada mais é do que um momento burocrático para a proteção legal das grandes empresas, e que não expressa realmente uma plena concordância com os termos ali postos, muito menos pode se pressupor que os usuários conheçam realmente todas as questões envolvendo o mercado de dados que os envolve. Com isso pode-se dizer que os cidadãos, usuários das tecnologias de vigilância, são impotentes diante das empresas de vigilância, pois são incapazes de criar alterações no contrato para que seja mais próximo de seu interesse, e não possuem a liberdade real de recusar o contrato que lhes é imposto. Nestas circunstâncias, apenas restaria conviver com todas as mazelas e processos indesejáveis em troca de ter as necessidades várias supridas por essas empresas:

> Assim sendo, será inevitável concluir que se esta tendência cada vez maior em direção à ingerência na intimidade, não for controlada, em algumas décadas não haverá nenhuma preocupação sobre as questões envolvendo o conceito de privacidade, de intimidade, já que aceitaremos como um fato evidente que vivemos num aquário e que não somos homens livres, mas peixes (BAIÃO; GONÇALVES, 2014, p. 16 e 17).

Baião e Gonçalves não comparam a liberdade de hoje à de peixes simplesmente pela presença das novas tecnologias nas sociedades, mas sim porque, apesar de todas as diversas possibilidades muito benéficas que as tecnologias oferecem para toda a sociedade, inclusive em âmbito político, nenhuma dessas possibilidades surge sem um preço fundamental de ser considerado: a privacidade, a intimidade, a captura das experiências de vida, de personalidades, a um ainda pouco conhecido e regulado mercado de dados. O incontrato é um dos demonstrativos do caráter de inevitabilidade que a vigilância tem sobre os usuários, que se expressa em toda a impotência do indivíduo em relação a este fato que age sobre ele.

A partir destas considerações é possível compreender como os capitalistas de vigilância podem adquirir grandes lucros ao vender informações comportamentais sobre milhões de indivíduos, pois os que detêm o conhecimento sobre os comportamentos humanos podem ofertar o produto mais desejado no momento mais propício à venda. Assim, os capitalistas de vigilância garantem a receita de vigilância, o ganho monetário oriundo da venda de predições humanas. Nas palavras da autora:

> O capitalismo de vigilância começa com a descoberta do superávit comportamental. Mais dados comportamentais são transmitidos do que o necessário para melhorias nos serviços. Esse superávit alimenta a inteligência de máquina — o novo meio de produção — que gera predições do comportamento do usuário. Esses produtos são vendidos para empresas clientes em novos mercados futuros comportamentais. O ciclo de reinvestimento de valor comportamental é subordinado a esta nova lógica (ZUBOFF, 2021. p.77).

Zuboff afirma que um dos grandes triunfos dos capitalistas de vigilância foi estabelecer tecnologias dentro dos limites privados dos indivíduos, tendo acesso as suas casas e a conversas pessoais: "as tecnologias mais profundas são aquelas que desaparecem" (ZUBOFF, 2021). Ainda que as consequências dos mecanismos introduzidos na sociedade firam a esfera privada e pública, deleta-la da estrutura social passaria por grandes dificuldades, uma vez que são geradoras de necessidade. Os aparelhos utilizados para sequestro de dados têm suas funções significadas como não apenas eficientes, mas necessárias para a vida em sociedade. A necessidade dos indivíduos em relação a tais mecanismos se deve ao fato da reestruturação da sociedade ao receber determinada tecnologia: o acesso à internet transformou as estruturas da sociedade, o que faz com que seja difícil pensar o ordenamento social em sua ausência. A leitura desses aparelhos enquanto necessários por parte da sociedade é de grande importância para a segurança das receitas de vigilância: se são tidos como fundamentais para o ordenamento social, não seria coerente pensar em sua superação, portanto, qualquer mazela que venham a gerar pode ser muito mais facilmente aceita: "Nossa dependência está no cerne do projeto de vigilância comercial, no qual as necessidades que sentimos por uma vida eficaz lutam contra a inclinação de resistir às audazes incursões do sistema" (ZUBOFF, 2021, p.26).

Uma vez que tais tecnologias assumem posições na vida privada dos sujeitos, não é possível ao indivíduo ter pleno controle sobre quais dados estará fornecendo ao interagir no meio online. Pode-se imaginar, erroneamente, que o usuário poderia simplesmente usar os aparelhos de vigilância com cuidado com quais dados irá compartilhar, no entanto é importante frisar a existência do "texto sombra" que todo o comportamento carrega e que, por si, já impediria qualquer tentativa do indivíduo de filtrar o que é ou não compartilhado. Em outras palavras, não existe anonimato para os capitalistas de vigilância: todos os usuários estão em posição de fonte de dados, independentemente de quais comportamentos venham a ter.

O texto sombra é o dado que se encontra no texto fornecido, e que enriquecerá o estoque informacional contido; são os dados retirados dos comportamentos, os quais não estão disponíveis aos usuários, mas sim às máquinas. Sendo assim, os usuários enfrentariam dificuldade em filtrar quais dados estariam transmitindo, já que existe conhecimento técnico a disposição dos capitalistas de vigilância para tirar o melhor proveito de todas as ações. Tendo

em vista esses fatos é possível afirmar que, em alguma medida, o capitalismo de vigilância pode ferir a privacidade da população, que tem informações sobre si registradas e negociadas a despeito de seu consentimento ou conhecimento. A plena potência da capitalização de dados se sustenta, entre outros fatores, na evidente impotência de intervenção do sujeito sobre as operações na esfera digital, pois esta dimensão virtual não é se quer administrada pelo humano, ainda que seja feita para ele, o seu controle se mantém preservado pelas máquinas, cujo funcionamento é conhecido por poucos (MEIRELES, 2021).

O mercado de dados não teria ganho o espaço que tem hoje se não fosse o grande avanço tecnológico promovido pelas Big Techs para que isso acontecesse. As Big Techs podem ser entendidas como as grandes empresas de tecnologia localizadas, em sua expressiva maioria, nos Estados Unidos, e que exportam seus produtos para os mais diversos países do globo. Facebook, Apple, Microsoft, entre outras empresas somam-se ao que se entende por Big Techs. É uma característica destas empresas oferecer, de várias formas, mais liberdade, no entanto a fazem de forma bastante condicionada a garantia de que terão acesso aos dados dos usuários (MOROZOV, 2018). Morozov percebe que essas empresas ganharam tanto espaço que passaram a substituir o Estado para cumprir com uma série de demandas, além de deslegitimar as possíveis formas reguladoras que os Estados possam manifestar contra as vontades destas empresas, por exemplo:

> O aparecimento da Uber como repositório útil de dados, que nenhum planejador urbano pode dispensar, é algo alinhado à ideologia mais ampla do "solucionismo" adotada pelo Vale do Silício. As empresas de tecnologia, depois de apossarem de um dos mais preciosos recursos contemporâneos – os dados-, agora têm influência sobre os governos sem dinheiro e sem imaginação e podem, assim, se vender como salvadoras inevitáveis e benevolentes aos burocratas inertes das administrações municipais (MOROZOV, 2018, p.62).

Uber, Facebook, Microsoft, são algumas das grandes empresas que se entranham em, cada vez mais, territórios e abrangem a sua lógica de mercado para mais pessoas, enquanto os Estados não têm poder para frear estes avanços, e, com a demanda da população sobre as ferramentas trazidas por essas empresas cada vez mais alta, forma-se um cenário muito propício a um crescimento muito pouco limitado por parte das Big Techs. Isto não significa que as Big Techs desejem livrar-se totalmente da operação dos Estados, apenas de suas intenções reguladoras, visto que os Estados, além de clientes, são necessários para resguardar essa busca incessante por dados. Os Estados ainda ficam muito menos sobrecarregados na medida em que os aplicativos das empresas assumem tarefas sociais, o que é muito interessante considerando os momentos de grande escassez de recurso que o setor público pode apresentar. Ao invés de

se desenvolver um complexo sistema de saúde pública, por exemplo, o Estado pode aceitar que aplicativos voltados para a área da saúde desenvolvam tecnologias de monitoramento que sejam capazes de suprir as necessidades dos cidadãos. A mesma lógica poderia se aplicar para a área da educação, e outras (MOROZOV, 2018). Desta forma, o papel do Estado enquanto provedor de um bem estar social é cedida para empresas que passam a gerir os problemas sociais:

> Nossos maus hábitos podem ser detectados, analisados e corrigidos em tempo real, dissolvendo muitos dos problemas que hoje sobrecarregam os serviços sociais. Assim, a noção de política como um empreendimento comunitário se metaforsea num espetáculo individualista e favorável ao consumidor, em que as soluções- que agora chamamos de aplicativos- são buscadas no mercado, e não na praça pública (MOROZOV, 2018, p.114).

É preciso notar que quando uma empresa privada assume responsabilidades antes dadas ao poder público, as necessidades sociais passam a estar condicionadas às normas de mercado, o que quer dizer que a população poderá suprir sua necessidade na condição de consumidor de mercadoria, em outras palavras, serviços sociais tornam-se acessíveis mediante o poder de compra de cada cidadão enquanto indivíduo. Como começa a ficar evidente, quem mais sofre dentro dessa lógica são os mais pobres, que dependeriam de bons sistemas públicos de saúde, educação, transporte entre outros, e, caso não tenham poder de suprir suas demandas a partir do mercado, estarão desamparadas. Como os Estados estão enfraquecidos e as empresas estão mais preocupadas com as parcelas da população com maior poder de compra, criou-se uma narrativa em torno da pobreza enquanto resultado da falta de capacidade da própria pessoa pobre, e que, assim como o estado de pobreza é fruto do próprio indivíduo, é ele mesmo quem deve superá-la, como coloca Morozov:

> Os pobres tomam decisões financeiras ruins porque as outras preocupações reduzem sua "banda larga cognitiva", de maneira parecida com o uso do Skype ou do Spotify, que podem deixar sua conexão com a internet mais lenta. Segundo essa concepção, se os pobres recebessem uma mensagem de texto adequada no momento certo, eles poderiam acabar poupando mais. Para combater a pobreza, então, devemos ter "um ambiente isolado da escassez", de modo que as decisões ruins e irracionais sejam evitadas ou minimizadas por meio de algum sistema de monitoramento permanente (MOROZOV, 2018, p.109).

A interpretação da condição de pobreza como consequência das capacidades individuais deslegitima leituras mais sociológicas sobre a questão, e fazem propor como solução para as questões relacionadas à pobreza uma espécie de potencialização da pessoa pobre para abandonar este estado, isto é, cabe a pessoa pobre ser protagonista de sua própria vida e superar as adversidades sociais. A solução, portanto, não passaria pela readequação dos Estados para o enfrentamento aos problemas públicos, caberia a cada um lidar com as suas próprias dificuldades.

3. Neoliberalismo e capitalismo de vigilância

O protagonismo do indivíduo em relação à sociedade é uma das características da ideologia neoliberal, que pautou todo o desenvolvimento do capitalismo de vigilância. O neoliberalismo surge no cenário pós-segunda guerra mundial como uma resposta às políticas intervencionistas e ao próprio poder dos Estados, emergindo, na década de 1970, como modelo de administração em vários países, como Estados Unidos e Inglaterra, sendo elaborado, também neste momento, o Conselho de Washington, que colaborou para a disseminação do pensamento neoliberal em vários países (PAULANI, 2016). O pensamento neoliberal, ao contrário do liberalismo propriamente, não possui compromissos com a defesa de qualquer democracia, pelo contrário, busca-se defender um Estado capaz de atender e proteger os interesses de mercado, sem permitir que haja interferência da vontade popular sobre os processos garantidores de lucro (BROWN, 2019). Esta finalidade do Estado e o não cuidado com a democracia se deve, entre outros motivos, pela compreensão do termo "sociedade" como infundado, ou então, dos riscos que se constroem ao se supor sua existência. Hayek entende os indivíduos como detentores de liberdade individual, e o mercado como espaço para expressão de liberdade, a qual é, em certa medida, sacrificada para a formação de uma solidariedade e justiça social, ou seja, a sociedade é uma inimiga da liberdade, bem como a democracia, enquanto o mercado é tido como fundamental a ela. Assumindo esta oposição entre Estado e mercado, em que o primeiro ataca a liberdade enquanto o segundo a garante, é que se legitima o avanço do mercado por esferas da vida que antes pareciam inalcançáveis a ele.

Em termos neoliberais, o Estado deveria apenas permitir que o mercado agisse, produzindo e distribuindo mercadoria, sem a elaboração de planos de segurança ou estabilidade social; a única certeza deveria ser a do mercado, que atua para atender da melhor forma as demandas dos indivíduos, que agem racionalmente em busca de atender seus interesses próprios (PEREIRA, 2009). A desconstrução do conceito de sociedade é o que permite a esta ideologia ser a ideologia da plenitude do indivíduo, pois é na sociedade, e em especial nas sociedades democráticas, que se expressam as relações de interdependência, que exigem a elaboração de valores como justiça e respeito ao outro, que ultrapassam os códigos mercadológicos. Como a sociedade e os valores que a formam como unidade são tidos como empecilhos ao mercado, cabe então a ele extingui-lo para que se forme uma nova sociedade, individualista e antidemocrática, com um Estado potente e pronto para desarticular as dificuldades que poderiam ser impostas aos mercados:

> Nenhum intelectual neoliberal buscava um Estado fraco. O contrário, o objetivo duplo era limitar o escopo e focar acentuadamente o funcionamento do Estado (...) os neoliberais procuravam construir, consolidar e amarrar um Estado unificado e forte, um Estado no qual a soberania política significa desunir, a democracia, desorientar e dividir, e a burocracia exaurir" (BROWN, 2019, p.77)

Se disse anteriormente que uma das consequências da expansão do papel das tecnologias de vigilância para responder às demandas sociais é o condicionamento do serviço social enquanto mercadoria e do cidadão enquanto consumidor, significa dizer que o que era um problema social, passível de ser solucionado pelas vias do Estado, passa a ser tido como um problema de indivíduos, que assumem a posição de compradores. Isto quer dizer que está desconfigurado o caráter social da própria sociedade neoliberal, pois o social foi reduzido a um grupo de indivíduos compradores, e o bem público foi transformado em uma mercadoria. Essa transformação é fundamental para que se entenda como o capitalismo de vigilância avançou de forma tão abrangente pelo mundo: isso se deu na medida em que vários países assumiram a lógica mercadológica em contraponto a lógica das políticas públicas e dos direitos.

Existe, ainda, outra dificuldade dos Estados em lidar com a problemática do mercado de dados globalizado: o seu caráter transnacional. Ainda que existam acordos entre Estados, estes ainda tem sua atuação um tanto limitada às fronteiras territoriais, o que não é o caso das grandes empresas de tecnologia, que atuam simultaneamente em diversos países, de forma que políticas nacionais podem ser efetivas no controle de Big Techs, mas apenas em certa medida e dentro de um certo território limitado, limite este que já foi superado pelas empresas de tecnologia. Enquanto os Estado nacionais formaram-se e se consolidaram a partir de instituições nacionalizadas, as Big Techs se constituíram como profundamente transnacionais, dentro do fenômeno da globalização:

> As empresas, corporações e conglomerados transnacionais, em suas redes e alianças, em seus planejamentos sofisticados, operando em escala regional, continental e global, dispõem de condições para impor-se aos diferentes regimes políticos, às diversas estruturas estatais, aos distintos projetos nacionais (IANNI, 1994, p.152)

Existe ainda um fator desestimulante sobre os Estados quanto a limitar as operações das Big Techs em seus territórios: as instituições do mercado, por serem grandes detentoras de capital, são capazes de exercer influência sobre os países nos quais operam, o que causa uma disparidade de poder: os países que restringem essas empresas restringem também o emprego de capital feito por elas em seus territórios, o que significa que problemas antes herdados por essas empresas voltam a estar circunscritos aos Estados nacionais, além disso, as empresas em

si podem sempre voltar-se a outros países que não imponham regulações eficientes (BECK, 2011).

Pode se compreender a relação entre o pensamento neoliberal e o desenvolvimento do capitalismo de vigilância: apenas é possível desenvolver esta nova face do acúmulo de lucro uma vez que se legitima a exploração da experiência a partir de tecnologia desenvolvida para isto, e, sendo o mercado o melhor em produzir e distribuir recursos, torna-se, nesta lógica, difícil de questionar as ações realizadas por ele, pois se assume o bem do mercado como o bem da sociedade, de forma que questiona-lo equivaleria a questionar o bem comum. Em outras palavras, a ideologia neoliberal não permite pensar a sociedade se não a partir do indivíduo e do mercado; categorias como sociedade, democracia e Estado democrático ocupam o espaço de antagonistas em relação ao progresso comum ofertado pelas empresas, as quais podem, inclusive, vigiar os indivíduos e capturar seus dados para ofertar serviços mais precisamente personalizados e, como já ficou evidente, lucrar a partir destes dados.

Levar em consideração o pensamento neoliberal é fundamental para que se compreenda o capitalismo de vigilância, pois é o pensamento que preconizou este fenômeno (ZUBOFF, 2021), e que estabelece uma forma de pensar a relação entre mercado e Estado que se disseminou pelo mundo principalmente a partir da década de 1990 (HARVEY, 2008). Cabe apontar ainda que, apesar de nem o capitalismo de vigilância nem o pensamento neoliberal terem surgido no Brasil, num mundo globalizado que opera em redes transnacionais, todos os países, e o Brasil, são impactados pela lógica neoliberal e pelas transformações impostas pelo capitalismo de vigilância.

3.1 Laços de colonialidade

Para entender as relações entre os países do sul global, como o Brasil, e os países do norte, em especial os Estados Unidos, no contexto de capitalização dos dados, muitos autores recorreram ao conceito “colonialismo de dados” para se referir a este momento histórico no qual empresas de países que dominam as produções tecnológicas usam de suas tecnologias para capitalizar os dados coletados dos cidadãos de outros países:

> Os pesquisadores Nick Couldry e Ulises Mejias utilizaram a expressão colonialismo de dados para caracterizar esse momento de conversão dos fluxos da vida em uma torrente de dados, abrindo um período de uma nova fase de acumulação do capital. Assim, o colonialismo de dados seria tão relevante para o capitalismo na atualidade como foi o colonialismo histórico para a expansão do capitalismo mercantil europeu e sua transição para o capitalismo industrial.” (SILVEIRA, 2021. p.24).

Como Zuboff (2021) assinala, o que configura o capitalismo de vigilância como um novo momento econômico do sistema capitalista é a capitalização dos dados por parte das empresas, e é importante perceber que tais empresas não estão dispersas pelo mundo, não existem empresas brasileiras, por exemplo, que lucram com o comércio de dados referentes a população estadunidense. O fluxo de dados é unidirecional: os países do sul são vigiados e certos países do norte lucram com o produto da vigilância (SILVEIRA, 2021), e é o caráter unidirecional do fluxo de dados somado à interdependência dos países do Sul em relação as tecnologias providas pelo Norte que faz justificar tal relação política como colonial (SILVEIRA, 2021; QUIJANO, 2022). Como assinala Quijano (2022), ao adentrarmos o século XXI, ainda que se tenham desenvolvido democracias em diversos países do globo (sendo o Brasil um deles, ao abandonar a ditadura militar e estabelecer uma constituição de princípios democráticos), não deixa de existir uma configuração das relações de poder que priorize o que se pode chamar de países do centro, estes sendo da Europa e os Estados Unidos. Em outras palavras ainda, a democratização dos países colonizados não significou a extinção dos laços de colonialidade. Esta concentração massiva de dados no território estadunidense cria uma grande relação de dependência dos outros países em relação aos Estados Unidos, que, por serem meros pontos de extração de dados, estão impossibilitados de fazer do mercado global de dados lucrativo para si. Assim, o mercado global de dados reduz diversos países do globo, em especial os do sul, a localidades para a extração de dados e consumidores de tecnologias de vigilância, enquanto outros países, como o Estados Unidos, são acumuladores destes dados extraídos e dos recursos providos a partir deles.

Esta grande dependência dos países, especialmente os do sul global, em relação aos Estados Unidos, faz com que as políticas públicas desses países estejam comumente condicionadas ao uso de tecnologia estadunidense em seu território. Como aponta o exemplo posto por Silveira:

> SouGov utiliza a solução de central de ajuda (chat), denominada SerproBot, que utiliza tecnologia da empresa IBM – International Business Machines. Nesse contexto, o usuário fica ciente de que os dados digitados no chat poderão ser transferidos internacionalmente e ficam armazenados na infraestrutura da empresa por um período de 30 (trinta) dias. Após este período os dados são excluídos em definitivo. Tal armazenamento tem o objetivo de prover o aprendizado de máquina da ferramenta de chat denominada "Watson", onde as interações dos usuários no chat são utilizadas para "aprendizado" pelo computador que envia as respostas automáticas quando o usuário está sendo atendido por meio do chat do serviço SouGov. (SILVEIRA, 2021. p.26).

O caso relatado acima mostra como uma ferramenta provida pelo Estado brasileiro para seus cidadãos, por ser fruto de uma colaboração com uma empresa de tecnologia norte

americana, tornou-se instrumento de coleta de dados para serem utilizados pela empresa norte americana, e não pelo Estado brasileiro. O uso das plataformas digitais para a efetivação de ações do Estado brasileiro pode ser problemático não apenas pela inserção de tecnologias de empresas privadas como fundamentais, mas também pela ineficiência que pode gerar em uma política pública. Foi isto que foi demonstrado na seguinte situação:

> Um estudo realizado pela Rede de Pesquisa Solidária da Universidade de São Paulo (USP) revelou que, durante a pandemia de Covid-19, 7 milhões de pessoas em situação de pobreza ou extrema pobreza no Brasil não tiveram a garantia do auxílio emergencial por dois motivos principais: ausência de conexão à internet e, no caso das que tinham acesso, dificuldades no uso do aplicativo da Caixa Econômica Federal (BERNARDES; SOUZA, 2024)

A presunção de que uma ação governamental mediada por tecnologias digitais para pessoas de baixo poder aquisitivo será eficiente pode ser consequência de uma falsa percepção de que as tecnologias digitais de vigilância estão democraticamente distribuídas, de tal forma que estão aptas a serem mediadoras de ações de enfrentamento a problemas públicos de amplo alcance. De fato, os aparelhos digitais já se encontram consideravelmente distribuídos entre os indivíduos, mas milhões de brasileiros ainda não tem expressivo acesso a elas ou as suas funcionalidades, as afastando dos benefícios que seriam seus por direito. Desta forma pode se dizer que a dependência do Estado brasileiro sobre as tecnologias digitais para efetivação de suas ações torna-se problemática para o sucesso de determinadas políticas públicas, como no caso expresso acima, além de demarcar uma forma de colonialismo de dados (SILVEIRA, 2021).

Sobre as condições coloniais postas neste cenário é importante notar que:

> As corporações exploram a 'terra digital' por meio da extração de dados, semelhante à forma como as potências coloniais exploravam terras por recursos naturais. Esta exploração de dados não é apenas uma violação da privacidade individual, mas também uma forma de opressão econômica, onde a riqueza é criada para poucos à custa de muitos. Além disso, é fundamental ressaltar o papel que os dados científicos desempenham neste contexto. Dados coletados para pesquisa e descoberta científica são frequentemente apropriados por empresas privadas para seu próprio uso comercial. Isso transforma a ciência em uma ferramenta de colonização de dados, onde o conhecimento é monopolizado em benefício de uma pequena elite. O capitalismo de dados, portanto, se baseia na apropriação e exploração de dados científicos, assim como o colonialismo histórico se baseava na exploração de recursos naturais (SILVA, 2023, p.76)

O uso de tecnologias de vigilância em larga escala também é um dos requisitos para o desenvolvimento das chamas *smart cities*, que seriam cidades preenchidas de tecnologias capazes de melhorar a vida dos cidadãos que vivem nela, seja provendo melhores transportes, mais segurança, saúde, entre outros serviços.

> A proposta mercadológica das smart cities inclui soluções tecnológicas desenvolvidas para "lugar nenhum", ou seja, genéricas e que desconsideram elementos históricos e constitucionais de um espaço, como cultura, conflitos, populações etc. Outro ponto relevante é que os discursos se baseiam no que a cidade pode vir a ser, com um apelo ao futuro abstrato. Outros elementos que compõem a proposta corporativa de smart cities são: o pacote tecnológico genérico; a reafirmação das empresas de que a tecnologia é neutra; soluções proprietárias que tornam a cidade dependente das empresas; e alinhamento aos propósitos neoliberais (SCHIAVI, 2021, p.152 e 153)

O desenvolvimento das smart cities incorre, portanto, na ainda maior expansão das empresas de tecnologia, que passam a ter maior poder operacional na cidade e ampliam, com isso, os laços de dependência das cidades com as empresas privadas, realçando ainda mais o acúmulo de poder nas empresas em detrimento do Estado, expandindo a solução de problemas a partir do mercado ao invés das vias democráticas. Elas também concretizam que não é necessário efetivamente possuir um aparelho de vigilância para estar submetido a ele: uma vez que elas estejam postas amplamente no espaço público, o mero convívio neles já traz a condição de vigiado para os que se utilizam do espaço público. Pode se imaginar que as *smart cities* sejam um objeto de sociedade totalitário pela constante vigilância sobre os indivíduos a despeito de sua vontade, No entanto, para a autora, o capitalismo de vigilância avança como um poder não totalizante, pois não incorre em delimitações ideológicas ou mesmo de comportamento, as pessoas agem com certa liberdade para decidir como fazer, e é importante que seja assim para que as informações coletadas se aproximem o máximo do real, em outras palavras, o capitalismo de vigilância não carrega a pretensão de fazer com que as sociedades na qual existe sejam iguais em pensamento e forma de ser, mas sim genuínas em suas experiências observáveis. Importante frisar que o limite para esta liberdade de comportamento e pensamento se restringe aqueles que são coniventes com o capitalismo de vigilância, ou seja, que não sejam tidos como ameaçadores a ele, mas, como vem se mostrando, os indivíduos tem pouco ou nenhum poder efetivo em deter as intenções vigilantes.

3.2 O mercado de dados e a venda de democracia

O mercado global de dados permite a potencialização da venda das mais diversas mercadorias a partir da modulação algorítmica, inclusive a compra e venda da potencialização de campanhas políticas muito eficientes em definir resultados eleitorais mesmo a nível federal. Em outras palavras, nem mesmo resultados eleitorais deixam de sofrer consequências diretas causadas pela modulação algorítmica. Um dos casos que mais repercutiu nos últimos anos envolvendo a relação dos algoritmos com resultados eleitorais foi a eleição presidencial dos Estados Unidos em 2016, que terminou com a eleição do candidato ícone da direita

estadunidense, Donald Trump[5]. Para vencer as eleições, na ocasião, a campanha de Trump voltou-se à comunicação nos meios digitais, e, para isso, contrataram uma famosa empresa da época que se tornaria famosa por mover diversas campanhas eleitorais pelo mundo, chamada Cambridge Analytica, que era uma empresa estadunidense voltada para o uso de dados para elaborar campanhas eleitorais eficientes, mais especificamente com os uso das plataformas digitais.

Para realizar a campanha de Donald Trump, a empresa Cambridge Analytica optou por fazer um contrato com a empresa Facebook Inc., que divulgaria diversos materiais eleitorais a seus usuários a partir dos dados que possuía sobre cada um. Alexander Nix, que foi CEO da empresa durante a campanha de Trump, alega ser capaz de prever e influenciar os comportamentos dos usuários a partir dos traços de personalidade identificados a partir dos dados armazenados sobre cada um, e, influenciando os comportamentos, se pode influenciar o voto (AMER; NOUJAIM, 2019). É justamente o conhecimento sobre a personalidade dos eleitores que elevariam a eficiência da campanha eleitoral das redes. A partir dos dados disponibilizados pelo Facebook, a empresa Cambridge Analytica pôde disponibilizar conteúdos precisos para convencer cada eleitor, a partir de suas crenças pessoais, de que deveria votar em Donald Trump (AMER; NOUJAIM, 2019). A campanha se mostrou eficiente, apesar de Trump ter menos votos no total em relação a sua oponente, o sistema eleitoral americano estabeleceu sua vitória (BBC, 2019). A mesma empresa foi contratada para trabalhar nas campanhas políticas pró Brexit, que requeriam a saída da Inglaterra da União Europeia, campanha que também foi bem sucedida.

Apesar do sucesso promovido pela Cambridge Analytica a seus clientes, houve indignação por parte da população ao ter contato com a forma operacional da empresa, uma vez que não havia o conhecimento comum de que seus dados poderiam ser usados da forma como foram. Em 2018 a empresa encerrou suas operações e entrou com pedido de falência após as repercuções envolvendo a forma como agiu durante as campanhas eleitorais dos Estados Unidos em 2016. O documentário mostra como bastava uma pessoa ter uma conta registrada nos sistemas da empresa Facebook para que seus dados estivessem plenamente disponíveis para uso de promoção de campanhas eleitorais[6]. Os Estados Unidos e a Inglaterra não foram os únicos países a terem resultados eleitorais fortemente influenciados por mecanismos de

[5] Em 2024, Donald Trumo foi reeleito presidente dos Estados Unidos. Superando sua adversária política, Kamala Harris (BBC, 2024).
[6] O documentário em questão. chamado Privacidade Hackeada, está disponível na plataforma digital Netflix

modulação comportamental. Carole Cadwalland, jornalista e ativista por direitos referentes aos dados, ressalta como o Whatsapp, plataforma de interação virtual da Facebook Inc. foi fundamental para a campanha política do candidato Jair Bolsonaro no Brasil (AMER; NOUJAIM, 2019), que foi eleito em sua primeira disputa eleitoral para a presidência. Apesar das eleições presidenciais dos Estados Unidos em 2016 e a do Brasil em 2018 terem sido marcadas pela ampla utilização das redes sociais, com certeza não foram as únicas.

Em 2010, pesquisadores do Facebook realizaram uma pesquisa a fim de medir a capacidade de influência da rede social sobre os eleitores: dois grupos receberam uma publicação na qual exibia o local de votação da pessoa e um botão virtual escrito “eu votei”, um dos grupos recebia ainda uma lista de até seis amigos que haviam clicado neste botão, o outro grupo não recebia tal lista; existiu ainda um terceiro grupo o qual não recebeu essa publicação. Os pesquisadores acreditam que esta publicação levou 340 mil pessoas a irem as urnas, sendo especialmente eficiente sobre o grupo que tinha acesso a lista de amigos que haviam clicado no botão “eu votei” (ZUBOFF, 2021, p. 446 apud BOND, R.M. et al. 2012).

Estes casos mostram como o capitalismo de vigilância pode ser uma grande ameaça às democracias pelo mundo. Conhecer o perfil dos eleitores e poder apresentar conteúdos direcionados de forma a potencialmente alterar ou reforçar um pensamento político atinge diretamente resultados eleitorais, ainda mais se os mecanismos que permitem estas alterações de comportamento não são regulados, ou sequer conhecidos. Os meios digitais, as redes sociais e as tecnologias de vigilância como um todo podem se apresentar como imparciais, técnicas e inofensivas politicamente, mas se as eleições de países democráticos estão sendo afetadas negativamente por tais tecnologias, então é preciso considerar suas operações e pensar formas de evitar o antagonismo entre democracias e capitalismo de vigilância.

Não apenas as escolhas eleitorais, mas as escolhas em geral estão abarcadas pelo imperativo da predileção; não se pode dizer que as escolhas dos usuários são realmente suas, já que sempre estão sendo instigados por uma série de estímulos comerciais sobre seu comportamento. De certa forma, pode-se dizer que o imperativo de predileção fere o próprio planejamento dos usuários quanto ao futuro: só se pode querer e planejar dentro do que está estabelecido a partir das constantes influências, não há espaço para desejos e planejamentos que não estejam alinhados com uma certeza de consumo: o que se deseja deve expressar uma vontade de consumir um produto, o qual será ofertado no tempo certo a partir de ações algorítmicas. Para Zuboff (2021) a consequência da modulação algorítmica é a violação ao direito de escolher um planejamento futuro. Para a autora, planejamentos são tentativas de

estabelecer certezas em relação ao futuro, ou seja, uma tentativa de estabelecer ordem em algum nível diante de um futuro amplamente desconhecido. Como o capitalismo de vigilância pauta-se pela certeza de comportamentos (do consumo de aparelhos de vigilância, da entrega de dados, da eficiência do marketing direcionado) não cabe mais aos usuários estabelecer o que fazer e como interagir com as tecnologias: há uma predeterminação, um imperativo de certeza. Por este motivo Bogard (1996) considera os processos preditivos como geradores de "biografias futuras", pois os perfis dos usuários são o que permitem estabelecer certezas sobre os comportamentos deles (BRUNO, 2008 apud BOGARD, 1996). O imperativo preditivo fere, portanto: "o sacrifício do nosso direito ao tempo futuro, que compreende a nossa vontade de ter vontade, autonomia, direitos de escolha, privacidade e, no fundo, nossa natureza humana" (ZUBOFF, 2021. p.516).

Pode-se afirmar que a elaboração de políticas públicas voltadas à proteção dos usuários se mostra fundamental para a preservação das liberdades de escolha e para a sustentação dos sistemas democráticos, já que, muito mais do que controlar o que a população irá consumir, os dados permitem modular em quem os usuários irão votar (AMER; NOUJAIM, 2019). Morozov também percebe que um dos custos do capitalismo de vigilância seja a própria democracia, e conclui:

> A tentação da política baseada na IA é evidente: é barata, limpa e supostamente pós-ideológica. O custo, no entanto, pode ser a própria democracia e, a menos que a Siri ou a Alexa passem a refletir sobre a política da memória e as formas de lidar com a injustiça histórica, não parece que vale a pena pagar esse preço para ter menos buracos nas ruas (MOROZOV, 2018, p.143).

Assumir que as grandes empresas de tecnologia possuem a competência necessária para lidar com as questões sociais, por possuírem os aparatos técnicos para isso, possui, entre outras consequências, um grande aumento do poder dessas empresas sobre a sociedade como um todo. A cada vez maior presença dessas empresas na vida dos cidadãos anuncia o quão poderosas elas se tornam para defender os seus interesses, pois, como se pode perceber pelo que foi anunciado até o momento, tais empresas, tendo o controle dessas tecnologias, de suas possibilidades de uso, controlam também a própria vivência dos cidadãos que de dá a partir delas. Neste sentido, pode se dizer que há uma dominação das grandes empresas de tecnologia em relação aos cidadãos, tendo a vigilância como importante ferramenta na manutenção desta condição[7].

[7] A recente decisão anunciada por Mark Zuckemberg de retirar das plataformas Facebook e Instagram a checagem independente de fatos reitera o dominínio de tais empresas, por exemplificar o uso do poder para limitar ações que distõem dos princípios e interesses que guiam as grandes empresas de tecnologia (BBC, 2025).

3.3 Relações de poder e dominação

Morozov (2018) aponta, com razão, que as IAs podem ser apenas supostamente consideradas pós-ideologias. À medida que se assume as estruturas de poder no plano internacional, esta condição de "pós-ideológica" torna-se bastante questionável. As relações de poder que se desenvolvem a partir dos mecanismos de vigilância se traduzem não apenas nas configurações de sociedade disciplinar ou de controle, mas acarretam também níveis de hierarquia no plano internacional entre países. Muitos autores utilizaram-se do conceito de hegemonia para entender as relações de poder no plano internacional. Leornardo Ramos e Geraldo Zahran relembram que:

> Deve-se notar que, quando Gramsci fala da hegemonia como "direção intelectual e moral", afirma que essa direção deve ser exercida no campo das ideias e da cultura, manifestando, assim, a capacidade de conquistar o consenso e de formar uma base social, já que há direção política sem consenso. É importante notar ainda que a hegemonia cria, também, a subalternidade de outros grupos sociais, subalternidade essa que não se refere apenas à submissão à força, mas também às ideias. Não se pode, em hipótese alguma, perder de vista que a classe dominante repassa a sua ideologia e realiza o controle do consenso por meio de uma rede articulada de instituições culturais que seriam os "aparelhos privados de hegemonia (RAMOS; ZAHRAN, 2006, p. 144)

O conceito de hegemonia permitiu às ciências sociais elaborar com mais sofisticação reflexões sobre as formas de dominação de classe para além das relações materiais. Como se coloca na citação acima, a hegemonia se sustenta a partir da dominação das ideias das classes dominantes em relação às dominadas, o que significa dizer que as ideias destas classes dominantes é que imperam sobre as demais. O poder hegemônico influi diretamente na cultura, nas visões de mundo, na compreensão dos dominados de sua posição em relação aos dominantes.

> Destarte, pode-se dizer que a hegemonia é isso: determinar os traços, as características, as peculiaridades específicas de uma determinada condição histórica, ou seja, de um determinado processo histórico. É tornar-se o protagonista por meio de um processo progressivo, de reivindicações que são de outros estratos sociais, unificando-os com parâmetros ideológicos e mantendo-os unidos. A hegemonia, portanto, não é apenas política, mas também um fato cultural, moral, enfim, de concepção de mundo (RAMOS; ZAHRAN, 2006, p.144).

Quando se utiliza do conceito de hegemonia para pensar o plano internacional, se conclui que a hegemonia é a dominação de um ou mais países em relação aos demais de forma a fazer prevalecer seus interesses. Não se trata aqui de uma dominação que se dá meramente a partir da disparidade de forças, mas que se dá a partir das relações políticas, econômicas e culturais, que estabelecem uma ordem internacional que prioriza os países dominantes. Esta transposição do pensamento gramsciano ao plano internacional foi feito por uma série de

autores anteriormente, os quais foram chamados “neogramscianos”, estes autores preocuparam-se em pensar as relações de poder brando (*soft power)* no plano internacional tendo como referência os pensamentos de Gramsci (PEREIRA, 2011). Pereira aponta que não se pode confundir poder brando com falta de poder, pois é o poder brando que estabelecerá a ordem vigente a partir do reconhecimento dos dominados sobre a condição do país dominante. Nesse sentido, uma série de artifícios são utilizados para a manutenção do poder brando, entre elas, as empresas multinacionais:

> As empresas multinacionais americanas preencheriam o papel dos exércitos na medida em que realizaram uma forma de dominação econômica similar ao dos impérios europeus, mas sem o recurso à anexação de territórios e populações. Além disso, os Estados Unidos construíram, ao lado da Europa ocidental e do Japão, uma ordem internacional baseada em instituições econômicas e políticas cuja operação dependeu da sua capacidade de liderar e formar um consenso mínimo no sistema internacional. O recurso ao conceito de hegemonia gramsciano novamente é fundamental para explicar essa ordem e sua importância nas relações internacionais do século XX, por formar-se fundamentada no consenso, não no recurso à força (PEREIRA, 2011, p.23)

A hegemonia se consolida, portanto, não necessariamente a partir de guerras entre Estados-nação, como as que ocorreram massivamente no século XX, mas sim através da sobreposição cultural e econômica de determinados países sobre outros, o qual se poderá sustentar uma vez que o dominante esteja relativamente aceito, pelos dominados, enquanto tal. O consenso em torno da estrutura de poder é o que permite que ela se mantenha. Nos limites desta pesquisa, é a legitimidade sobre a operação das grandes empresas de tecnologia que permite a elas usufruir de sua posição de poder e legitimidade que foram construídos historicamente e que pautaram-se no poder já estabelecido do país no qual muitas delas surgiram: o Estados Unidos. A posição de hegemonia dos Estados Unidos no plano internacional faz prevalecer suas estruturas para além de seu território, o que faz manter a ordem e o consenso em torno destas estruturas, sendo as empresas multinacionais uma delas. A hegemonia dos Estados Unidos se dá a partir de uma já existente condição de hegemonia de classe estabelecida dentro do território norte americano:

> o estabelecimento de uma hegemonia mundial é resultado de uma “expansão para o exterior” de uma hegemonia nacional estabelecida por uma classe dominante. (...) Por meio dessa expansão, é formada uma ordem mundial baseada na hegemonia de um Estado sobre os demais. A terceira condição é a expansão da hegemonia para os países periféricos, que incorporam alguns aspectos econômicos e culturais do “núcleo hegemônico” sem, no entanto, alterar, de modo significativo, seus regimes políticos. Por essa razão, o modo de produção capitalista expande-se para os países periféricos sem que, internamente, esses países modifiquem de modo substantivo as antigas estruturas de poder vigentes (PEREIRA, 2011, p.240).

Dito de outra forma, o país com poder hegemônico estabelece a ordem entre os países nas relações internacionais, dita quais países estão no centro das relações de poder e os que são

periféricos a ela. Para que esta ordem de poder se sustente, é preciso que os demais países incorporem o modo econômico e cultural do país dominante, de forma a aceitar tal dominação entre países sem que isto necessariamente faça alterar demasiadamente as relações de poder no interior dos países dominados. O que se tem, portanto, é um desequilíbrio de poder de certos países em relação a outros, no caso, dos países do norte, especialmente os Estados Unidos, em relação aos demais, especialmente em relação as do sul.

O capitalismo de vigilância reproduz esta condição de dominação entre países a partir das empresas multinacionais de tecnologia, que gerem uma dominação econômica, a partir dos lucros conquistados pelo acúmulo de dados e cultural ao estabelecer uma rotina social que exige aparelhos ofertados por estas empresas. O que se percebe, portanto, é que o avanço do capitalismo de vigilância aos mais diversos países apenas é bem sucedido na medida em que assume uma estrutura de poder no qual aqueles que se beneficiam diretamente dele possuem o poder e a legitimidade para disseminá-lo e fortalece-lo sem causar ampla indignação ou revolta em razão dos malefícios causados por ele[8].

Quijano (2022) aponta como o momento da globalização que se desenvolve no século XXI estabelece uma estrutura de fluxo de recursos do sul ao norte:

> 1.está em curso um processo de reconcentração do controle de recursos, bens e rendas nas mãos de uma minoria da espécie
>
> 2.O anterior implica que está em curso um processo de polarização social crescente da população mundial, entre uma minoria rica, proporcionalmente decrescente, mas cada vez mais rica, e a vasta maioria da espécie, proporcionalmente crescente e cada vez mais pobre" (QUIJANO, 2022, p.8)

O capitalismo de vigilância é uma forma da economia globalizada que implica não apenas uma desigualdade na distribuição de recursos, mas de poder, estendendo ainda mais as distâncias entre o sul e o norte global, no qual os países do sul se tornam cada vez menos autônomos e mais suscetíveis aos interesses dos países do norte global, em especial o Estados Unidos. Com isso, Quijano (2022) conclui que o próprio fenômeno da globalização, no qual se desenvolve o capitalismo de vigilância, se dá a partir de imposições dos países hegemônicos em relação aos dominados, estabelecendo, assim, novos laços de colonialidade, que, no século XXI, com o auxílio das tecnologias que permitem superar em alguma medida as limitações postas pelos territórios, se estenderam e se se tornaram mais complexas. Esta colonialidade do

mundo moderno é que pauta a negociação dos Estados nacionais sobre os limites de exploração dos países centrais em relação aos demais.

O poder hegemônico dos Estados Unidos e o poder das grandes empresas de tecnologia se sustentam mutuamente (PEREIRA, 2011; RAMOS; ZAHRAN, 2006), de forma que cabe aos demais países estabelecer limites, por meio de regulamentações legais, ao poder destas potências, isto é, os Estados Unidos e as organizações que usufruem de sua posição. No que diz respeito ao capitalismo de dados, coube aos países elaborarem regulamentações capazes de proteger os cidadãos contra os atos de poder vindos do norte. No Brasil, uma série de leis foram elaboradas, como o marco civil da internet e a LGDP, objeto de estudo desta pesquisa que será apresentada para que então possa ser estudada a partir das argumentações teóricas anteriores.

4. A lei 13.709/2018, contexto e implicações

A lei 13.709/2018 é fruto do projeto da lei (PL) 4.060/2012, apresentado pelo deputado Milton Moti, do partido republicano. O projeto apresentava vinte e cinco artigos, dos quais destacam-se os dois primeiros: "Art. 1º. Esta lei tem por objetivo garantir e proteger, no âmbito do tratamento de dados pessoais, a dignidade e os direitos fundamentais da pessoa natural, particularmente em relação a sua liberdade, privacidade, intimidade, honra e imagem; "Art. 2º. Toda pessoa tem direito a proteção de seus dados pessoais" (BRASIL, 2012).

Os objetivos do projeto se mantiveram até sua promulgação, que somente se deu em 2018. Entre 2012 e 2013 o projeto tramitou entre a Comissão de Ciência, Tecnologia e Inovação (CCTI) e a Coordenação de Comissões Permanentes (CCP). Ainda em 2012, o projeto foi somado ao projeto de lei 3558/2012, apresentado pelo deputado Armando Vigilio do Partido Social Democrático (PSD), que também tinha por intenção propor uma regulação da proteção de dados no país. O deputado Milton Toti requereu que seu projeto fosse desassociado do projeto de lei 3558/2012, pedido que fosse indeferido pela mesa diretora da Câmara dos Deputados, em 2013. Ainda em 2013, a mesa diretora encaminha à Comissão de Ciência, Tecnologia e Informação (CCTI) um pedido de revisão do indeferimento da desapensação entre os dois projetos de lei, cujo relator foi o deputado Nelson Merquezan Junior do Partido da Social Democracia Brasileira (PSDB). Esta revisão não foi concluída pois, em 2015, deu-se fim à legislatura na qual ambos os projetos haviam sido produzidos. Com isso, de acordo com o regimento interno da Câmara dos Deputados, ambos os projetos foram arquivados em janeiro de 2015.

Porém, já em fevereiro do mesmo ano houve o requerimento para o desarquivamento de uma série de projetos de leis da antiga legislatura, entre eles o projeto de lei 4.060 de 2012, o qual foi deferido pela mesa diretora ainda em fevereiro de 2015. O novo relator da lei, deputado Sergio Zveiter do Partido Social Democrático (PSD) convidou representantes de diversas instâncias relacionadas com o tema de que trata a lei: a Associação Brasileira de Agências de Publicidade (ABAP); Associação Brasileira de Marketing Direto (ABEMD) e Associação Brasileira das empresas de rádio e televisão (ABERT) para participarem de uma audiência pública. Ainda em 2015, outra audiência pública foi requerida com outros participantes, e outras audiências aconteceram ao longo de 2016. Em 22 de maio de 2018 o deputado Orlando Silva, do Partido Comunista Brasileiro (PCB) pede à mesa diretora para que o projeto de lei seja posto em caráter de urgência, sendo apreciado no dia 28 do mesmo mês, no dia seguinte o projeto entra em votação e é aprovado, sendo, em seguida, encaminhado ao Senado, que aprova o

projeto no dia 10 de julho de 2018; é sancionada pelo então presidente da república, Michael Temer e é publicado no diário oficial da União no dia 15 de agosto de 2018. Apesar de publicada em 2018, a lei apenas entra em vigor em 2020, por determinações que a própria lei apresenta.

A lei é uma em um extenso conjunto de legislações elaboradas pelo poder federal para estabelecer segurança, em sentido amplo, no meio digital. A lei do cadastro positivo, de 2011, e a código civil da internet, de 2014, mostram como já existia, anos antes da promulgação da LGPD, um trabalho legislativo em torno da coleta de dados na internet. Antes do sanção do Código Civil da Internet, existia um "vazio normativo", de forma que as instâncias jurídicas eram guiadas por interpretações de códigos anteriores, como o código do consumidor

> Normas estas que, em sua essência, no entanto, não tinham o condão de prover integralmente disciplina mínima e adequada em casos de conflitos de interesses, antinomia de regras, e tensão entre direitos subjetivos dos usuários e provedores da Internet (PADUA, 2018).

Apesar das leis que antecederam a LGPD, ainda faltava uma lei que tratasse especificamente do processo de acúmulo e tratamento de dados, especialmente em nível internacional, o que fez desta lei tão importante. Além disso, em 2016 a União Europeia oficializou um amplo regulamento sobre controle de dados, chamado GDPR, o que levou outros países a também avançar em suas legislações sobre este assunto, sendo o Brasil um deles, especialmente porque os países que não apresentassem legislações compatíveis a GDPR poderiam sofrer limitações em suas relações econômicas com os países da União Europeia (LUGATI; ALMEIDA, 2022; PINHEIRO, 2020).

4.1 Contexto de aprovação da LGPD

O ano de 2018 foi marcante para a história política do Brasil, não apenas pela aprovação da LGPD, mas por ter sido o ano da disputa eleitoral pela presidência do país entre Fernando Haddad, então candidato do Partido dos Trabalhadores (PT), e Jair Bolsonaro, candidato, naquele momento, do Partido Social Liberal (PSL). O pleito foi encerrado com a eleição de Bolsonaro, com 57.797.847 dos votos válidos (55,13%), enquanto seu concorrente teve 47.040.906 dos votos válidos (44,87%) (TSE, 2018; G1, 2018). O processo eleitoral daquele ano provocou uma série de discussões públicas em torno do modo como os meios tecnológicos foram usados naquele momento eleitoral. Em 2019, foi noticiado que empresas foram contratadas para efetuar disparos em massa via aplicativos de troca de mensagens com fins de convencer os eleitores brasileiros a se simpatizarem com Bolsonaro (VIEJO, 2019). As campanhas em favor de Haddad também foram acusadas de uso indevido das redes de compartilhamento de mensagem. Para apontar um caso específico, Bolsonaro moveu um

processo jurídico contra a campanha de Haddad por promover notícias falsas contra ele, pedindo então direito de resposta. Tal processo foi negado pela justiça brasileira por entender que o material divulgado pela campanha de Haddad não possuía caráter ofensivo (POMPEU, 2018). Ainda em 2018, segundo matéria da Câmara de Curitiba, foram produzidas seis fake news por dia, considerando apenas aquelas identificadas por agencias de checagem de fatos (GAMA, 2022), o que levou a autora a caracterizar o cenário como uma "guerra de desinformação".

A ampla divulgação de notícias falsas e os problemas políticos que elas traziam fez emergir um momento de grande preocupação sobre as eleições futuras, e deixou evidente aos legisladores brasileiros que era preciso definir com mais precisão limites de ação para as grandes empresas de tecnologia. Para citar alguns casos que evidenciam tal preocupação, em 2018 foi apresentado o projeto de lei 246/2018, que dispunha sobre medidas para combater a divulgação de notícias falsas na internet (Senado Federal, 2018). Em 2020 a Comissão de Constituição e Justiça analisou a criação de uma instituição independente de acompanhamento das mídias sociais, em conformação ao projeto de resolução do senado (PRS) 56/2019 (senadonotícias, 2020). Em 2022, o presidente da Tribunal Superior Eleitoral (TSE) Luiz Fux, reuniu-se com representantes de dez partidos políticos afim de firmarem uma colaboração contra a disseminação de notícias falsas (TRE-PA, 2022).

4.2 Método de análise da lei 13.709/2018 (LGPD)

Em 2018 foi publicada a lei 13.709/2018, chamada Lei Geral de Proteção de Dados, que seria responsável por atualizar o marco normativo nacional do Brasil referente àcoleta e uso de dados, tendo por função a proteção dos direitos fundamentais à liberdade e àprivacidade, antes previstos na Constituição Federal. Para que a análise da lei seja adequada a esta pesquisa, ela será focada nos mecanismos apresentados por ela para a proteção da privacidade do indivíduo em relação às grandes empresas de tecnologia, mas é importante ressaltar que a lei abrange também outras interações, como consta em seu Artigo 1º: "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018).

A lei é formada por 65 artigos divididos em dez capítulos. Para uma leitura abrangente da lei, a apresentação que se segue será dividida pela ordem dos capítulos, para que, ao fim, se possa discutir sobre sua relação com a capitalização de dados. A versão da lei analisada é a que

foidisponibilizada no dia 17 de abril de 2023, pois se priorizou a versão mais recente da lei em relação a sua forma original. Para a análise da lei buscar-se-á relacionar os artigos apresentados pela LGPD às características fundamentais do capitalismo de vigilância, resumidas na figura 4 a seguir , de forma a fazer entender a relação entre ambas e as alterações previstas em lei a tal fenômeno, sendo possível, assim, averiguar se a lei apresenta mecanismos capazes de defender os cidadãos e quão eficiente pode ser no sentido de frear os avanços do capitalismo de vigilância.

Figura 4- Características gerais do capitalismo de vigilância

Acúmulo ilimitado de dados	Para garantir sempre mais lucros é fundamental que as empresas não tenhamlimitações prévias sobre quantos dados podem coletar.
Capitalização de dados	Osdados coletados, que formarão o Big Data, devem ter expressivo valor de troca.
Integração das tecnologias de vigilância na sociedade como um todo	A coleta de dados se dá através das tecnologias com as quais os cidadãos não apenas convivem, mas geram relações de necessidade.
Incontrato	Não há uma expressiva possibilidade do cidadão declinar da oferta dos serviços e mercadorias ofertadas pelas Big Techs, justamente pela relação de necessidade estabelecida.
Colonialismo de dados	As condições geográficas e históricas nas quais se deu o desenvolvimento do capitalismo de dados estabelecem uma relação colonialista entre o sul e o norte global, em que os dados são acumulados nos países do norte, mais especificamente no Estados Unidos.
Divisão desigual da aprendizagem	O conhecimento referente àforma de funcionamento das tecnologias de coleta de

	dados é restrito a grupos específicos de trabalhadores com expertise para desenvolver e aprimorar as tecnologias de vigilância e acúmulo de dados a partir dos interesses das Big Techs.
Cidades inteligentes	As áreas urbanas são povoadas por tecnologias de vigilância as quais facilitam e expandem as possibilidades da captura de dados no espaço público.
Transnacionalidade	O mercado de dados não é um fenômeno limitado a apenas um país ou a um seleto grupo de países, mas é um fenômeno amplo que atravessa uma vasta variedade de países, o que significa uma dificuldade na sua regulação por parte dos Estados nacionais.

Fonte: conteúdo autoral

O artigo 10º e o artigo 12º da LGPD, que tratam do legítimo interesse e da anonimização de dados, terão seções específicas para serem tratados, isso por se entender que são especialmente relevantes para esta análise na medida em que estabelecem formas de legitimação da capitalização de dados sem a efetiva mediação do consentimento dos usuários ou de qualquer forma de expressão da vontade deles.

4.3 Disposições preliminares da LGPD

A lei, ao apresentar os princípios que a guiam, elenca mais de um princípio que apresenta a preocupação em relação à proteção dos dados dos usuários:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018).

Os fundamentos da disciplina de proteção de dados evidencia a preocupação dos legisladores em estabelecer uma lei que seja capaz de equilibrar a liberdade com inviolabilidade, de tal forma que, ao mesmo tempo que se assume uma liberdade de expressão, de informação, comunicação, a autodeterminação entre outros, não deixa de frisar a inviolabilidade da intimidade, da honra e da imagem, em outras palavras, ao se estabelecer as liberdades, se estabelece também condições e limitações para o exercício dela.

Este artigo, de certa forma, expressa uma busca por um equilíbrio que perpassará toda a lei entre o respeito aos direitos do cidadão e o desenvolvimento econômico e tecnológico com fins em inovação. Em certa medida, pode ser que ambos andem juntos, mas, em muitos casos, pode ser que se abra mão do respeito ao cidadão em função dos avanços tecnológicos. Toda a exposição anterior em torno do capitalismo de vigilância permite afirmar que, enquanto o mercado de dados leva ou busca levar a um maior desenvolvimento tecnológico com fins no lucro, há neste processo também uma violência contra os cidadãos, postos na condição de usuários fornecedores de dados. O artigo coloca como fundamento tanto a inviolabilidade dos direitos do cidadão, quanto a promoção do desenvolvimento tecnológico.

4.4 LGPD e os limites do capitalismo de vigilância

No artigo quinto e sexto, a lei apresenta uma série de conceitos que serão usados ao longo dela, sendo estes:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação,

> transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2018, artigo 5º).

Uma vez que estes dados são disponibilizados, a lei estabelece quais princípios serão fundamentais para o tratamento dos dados, que são:

> finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018, artigo 6º).

Percebe-se que os dois primeiros princípios, isto é, a finalidade e a adequação dizem respeito ao conhecimento de titular de dados sobre o tratamento, ou seja, o tratamento dos dados somente é legal na medida em que o seu titular teve a possiblidade de conhecer

previamente como se daria este tratamento. A lei enfatiza de tal forma a importância do conhecimento por parte do titular que os princípios de livre acesso, qualidade dos dados e transparência são todos princípios voltados para a integralidade da informação que deve alcançar os usuários, e sem os quais os primeiros princípios apresentados são comprometidos. Os princípios de segurança e prevenção se colocam como obrigações para que o tratamento de dados se dê de forma mais restrita a empresa envolvida, e o princípio de responsabilização e prestação de contas é fundamental para que as empresas de tecnologia que atuam com tratamento de dados sigam rigorosamente os demais princípios e a lei como um todo. O princípio da necessidade chama a atenção por reduzir, em muito, o escopo de acúmulo de dados das empresas, que, podendo apenas armazenar dados estritamente necessários, não poderão assumir ações desenfreadas em busca de acúmulo informacional indeterminado.

Todos estes princípios, por razões diferentes, se contrapõem às formas de operação do capitalismo de vigilância, isto porque todos estes princípios significam limites para a efetiva operação das empresas acumuladoras de dados. Certamente, estes princípios antagonizam com o acúmulo indeterminado de dados e com o incontrato. O incontrato é especialmente afetado pelo princípio do livre acesso, que coloca o cidadão na condição de conhecedor dos meios de tratamento de seus dados, e, portanto, mais capacitado para entender o que seu consentimento para com tais tratamentos significa. Ainda se mantém que os cidadãos possuem pouca autonomia para de fato recusar tais incontratos, mas, por este princípio, poderão ou deverão estar melhor informados pelas empresas.

Dadas as definições, a lei, no artigo sétimo, estabelece em quais circunstâncias o tratamento de dados poderá ser realizado:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e

> liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018, Artigo 7º)

A lei explicita que um critério mínimo para a possibilidade legal do tratamento de dados seja o consentimento do titular, isto é, pressupõe-se que o titular, diante dos conhecimentos que tem acerca da aceitação do compartilhamento de seus dados, recuse ou aceite este compartilhamento. Tal caráter legal remete ao conceito de "incontrato" antes apresentado, pois não há um diálogo entre partes para que se estabeleça a condição contratual entre elas, há apenas a imposição da parte empresarial sobre os usuários para que aceitem o compartilhamento de seus dados, caso contrário não será possível que acessem os serviços fornecidos por essas, e, como estes serviços assumem cada vez mais importância na vida dos cidadãos, recusa-los leva a exclusão daqueles que não aceitem os termos postos pelas empresas.

Nesta relação é que se expressa a assimetria entre as partes: enquanto as grandes empresas tecnologia gerenciam os dados dos usuários e estão em posição lucrativa no mercado global de dados, os usuários não apenas não administram tais dados como deles não possuem nenhuma fatia do lucro das empresas, o maior ganho dos usuários desta relação é poderem se manter enquanto usuários. Pode-se dizer que há uma assimetria de poder desconsiderada, neste momento, pela lei, pois coloca em certa igualdade as grandes empresas e seus usuários, uma vez que ambas aceitem as partes do contrato, ele é tido como legítimo. Este sentido da lei é reafirmado pela colocação do usuário como titular de dados, e que, enquanto titular, poderá oferta-los em troca dos serviços mediante contratação destes (FORNASIER; KNEBEL. 2021).

O artigo oitavo ainda estabelece como se dará o consentimento:

> O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os

> tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei. (BRASIL, 2018. Art.8)

O consentimento, portanto, deve ser expressivo nos termos do artigo, e não pode ser tido como fruto de um "vício de consentimento", é importante perceber também que o artigo formaliza uma possibilidade de revogação de consentimento, ainda que este tenha sido expresso nos termos da lei:

> A norma estabelece, então, que o fornecer do consentimento não significa a falta de interesse do indivíduo na tutela de suas informações pessoais, mas sim um ato de escolha garantida pela sua autodeterminação individual. Sob essa ótica, adquire grande relevância e constitui importante inovação a possibilidade de revogação do mesmo, prevista no art. 8º, §5º da lei. Tal prerrogativa é fundamental para fazer valer os direitos de liberdade e privacidade. Na legislação brasileira, a revogação é válida tanto para autorização para o tratamento, quanto em relação à circulação dos dado (FARIAS, 2020, p.51).

O inciso VI do caput do artigo 18, do qual o artigo trata, afirma o direitoà: "eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei" (BRASIL, 2018. Artigo 18 inciso VI). A exceção de que trata a lei é:

> Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018, artigo 16)

Chama a atenção o fato de que a lei não estabelece tempo limite para o armazenamento de dados, desde que sejam mantidos e obtidos legalmente, tendo, inclusive, como justificativa legal a sua transferência para terceiros. Desta forma, não parece existir um limite bem estipulado para o tratamento, nem para sua transmissão. A transferência dos dados, inclusive, ou o seu uso exclusivo, são justificativas legais para não excluir os dados ainda que o consentimento do titular seja retirado, o que sinaliza uma disparidade de poder de decisão entre as empresas e os cidadãos.

O artigo dezesseis, somado ao inciso quinto do artigo oitavo, manifestam um poder ao usuário antes inexistente: revogar o seu consentimento e ter a garantia a requerer a exclusão de

seus dados.A lei ainda especifica que tal revogação deve ocorrer sempre que o titular dos dados requerer, não sendo necessário que a empresa viole o contrato para tento. Apesar de tal medida permitir ao titular ter poder sobre seus dados mesmo depois de cedidos, a própria LGPD estabelece limites para este poder. Da forma como a lei está posta, as empresas tem plena capacidade para se protegerem contra pedidos de exclusão de dados e prolongarem a condição de mercadoria destes, em especial, caso os anonimize, isto é, desfaçam a relação existente entre o dado e o titular, ou então, reivindiquem que estão agindo em legítimo interesse.

O direito a pedido de exclusão de dados não é o único poder que a lei apresenta ao titular de dados, os artigos dezessete ao vinte apresentam direitos do titular fundamentais para o tratamento de seus dados, que são o direito à privacidade, liberdade e intimidade, nos termos da lei; confirmação do tratamento de seus dados, acesso aos dados, correção de dados incompletos, anonimização ou eliminação de dados tratados ilegalmente ou excessivos; conhecer a possibilidade de não conceder seus dados e as consequências disto e saber com quais entidades seus dados foram compartilhados (BRASIL, 2018). Os artigos dezenove ao vinte e dois dizem sobre a liberdade de acesso dos usuários sobre seus dados e os critérios utilizados para estabelecer um perfil de usuário, além de que o tratamento dos dados não pode ser usado para gerar prejuízo aos titulares, além disso, caso os dados que forem solicitados não forem fornecidos, o poder público poderá agir para averiguar se existe ação discriminatória por parte da empresa que trate os dados. A lei não estabelece o que pode ser entendido como prejuízo aos titulares e o que entende por uma ação discriminatória, mas deixa margem para que ambos esses tópicos sejam considerados problemáticos e possam ser motivo de mobilização pública em razão do titular de dados.

Todos estes artigos que se voltam para estabelecer plenas possibilidades de contestação por parte dos usuários sobre as ações dos agentes de mercado de dados vão contrapor-se ao acúmulo indeterminado de dados, pois, se o cidadão possui poder de se contrapor a como seus dados são utilizados ou acumulados, então não se poderá dizer que os dados são acumulados, com base na LGPD, indeterminadamente. Assim, tal qual os princípios anteriormente apresentados, o requerimento do consentimento surge como uma barreira para uma base do capitalismo de vigilância: acesso pleno a cada vez mais dados.

O capítulo quinto da lei estabelece como poderá se dar a transferência de dados do Brasil para os demais países, e ela estabelece que um dos pré-requisitos é que o país de origem também tenha medidas de proteção de dados similares aos desta lei, ou quando o controlador dos dados

provar que cumpre com todos os princípios apresentados nela. Existe, ainda, a prerrogativa de que os dados poderão ser transferidos se o titular de dados for previamente avisado sobre a operação e demonstrar acordo específico sobre ela. O artigo trinta e quatro estabelece que para que se possa averiguar se um país tem princípios legais compatíveis a esta lei, as autoridades públicas deverão observar: qual a natureza dos dados transferidos; quais os princípios de proteção de dados que regem sobre o país que receberá os dados; a adoção de medidas de segurança e de suporte jurídico e institucional para a proteção dos dados (BRASIL, 2018, capítulo V). Este capítulo fica responsável por estabelecer como a lei será efetivada nas relações internacionais, como se disse anteriormente, a dificuldade dos Estados nacionais em controlar a capitalização de dados se dá justamente na sua forma transnacional, enquanto os Estados têm seus poderes limitados territorialmente. Visto isso é que a lei apresenta formas de interagir com outros governos, estabelecendo até mesmo a ilegalidade da transição dos dados para um país que não apresente os mesmos princípios legais que os brasileiros. Por isso, pode-se dizer que a LGPD estipula uma reação a mais uma condição fundamental do capitalismo de vigilância, isto é, a transnacionalidade. Ao estabelecer a lei na relação com as regulações de demais países, busca-se uma expansão do poder regulador, feito a partir da cooperação de outros Estados, de forma a lidar com as questões transnacionais postas pelo mercado de dados.

A partir do artigo trinta e sete a lei volta-se as obrigações do controlador de dados e do operador de dados. Ambos os agentes são responsáveis pela efetivação da norma legal sobre o tratamento, sendo o controlador o responsável por estabelecer quais dados serão colhidos e para qual finalidade, enquanto o operador é o responsável pela efetivação do planejamento elaborado pelo controlador. A lei estabelece, em seu artigo quarenta e um, que os encarregados pelo tratamento dos dados deverão ter sua identidade tornada pública, e que cabe a estes receber as mensagens tanto dos titulares de dados quanto das autoridades oficiais. Em outras palavras, a lei estabelece cargos a serem ocupados pelos responsáveis pelo tratamento, para que observem o que a lei impõe, de forma que, de acordo com o artigo quarenta e dois, caso os agentes causem dano material ou moral a qualquer titular de dados, este deverá reparar os danos através de ressarcimento, desde que os danos tenham sido causados mediante comportamento em desacordo com a lei, além disso, pelo que define o artigo 44, caso os responsáveis pelo tratamento de dados deixem de assumir medidas de segurança esperadas pelo titular, estes responsáveis poderão responder pelo dano decorrente da insegurança de suas operações.

No caso de acidentes envolvendo o tratamento de dados, os agentes de tratamento são responsáveis por estabelecer ações efetivas de segurança para que isso não aconteça, assim como impedir que terceiros consigam o acesso aos dados de forma ilícita. Caso ocorra, é responsabilidade das agências de tratamento informar tanto às autoridades quanto aos titulares que forem lesados. Os agentes, nesta situação, ficam ainda encarregados de informar às autoridades: qual a natureza dos dados acessados ilegalmente; quais informações foram acessadas; como os agentes de tratamento tentaram evitar este acontecimento; quais outros riscos podem derivar desta falha; caso a comunicação não tenha sido imediata, o porquê; quais as medidas dos agentes de tratamento de dados para buscar reverter a situação. Além disso, é garantido às autoridades o poder de ampla divulgação sobre o ocorrido, caso se entenda que esta seja uma forma efetiva de proteger os cidadãos futuramente (BRASIL, 2018, artigos 46 ao artigo 49).

Os artigos cinquenta e cinquenta e um, que dizem sobre as boas práticas no tratamento de dados, estabelecem que cabe aos controladores e operadores de dados estabelecerem regras de boas práticas ao seu bom funcionamento legal, sendo que a lei não define exatamente quais regras deveriam ser essas. O que se estabelece é que o controlador de dados, observadas as especificidades de seu trabalho com os dados coletados, possui liberdade de implementar normativa que considere seu comprometimento para com “as boas práticas relativas à proteção de dados pessoais” (BRASIL, 2018, artigo 50, § 2º), além de outras características sobre como tal normativa poderia ser, em nenhum momento é imposto a obrigação de sua elaboração, apenas levantada a possibilidade dela.

O artigo cinquenta e dois, que trata das penalidades aplicáveis ao não cumprimento desta lei, apresenta multa, bloqueio de dados e exclusão de dados como possíveis penalidades as empresas, a depender da gravidade da infração, do grau do dano causado, sua reincidência e outros fatores, além disso, estabelece que caso o acesso ilícito dos dados se dê de forma individual, é possível que o controlador e o titular de dados entre em conciliação, e, uma vez que não se conciliem, as penalidades poderão ser aplicadas ao controlador dos dados.

A lei cria também um órgão público responsável pela fiscalização das boas práticas no âmbito do tratamento de dados, a chamada Autoridade Nacional de Proteção de Dados (ANPD), que é composta por cinco cargos que são preenchidos a partir das escolhas do presidente da república (BRASIL, 2018, artigo 58). A lei determina vinte e quatro funções à ANPD, entre elas:

> zelar pela proteção dos dados pessoais; zelar pela observação dos segredos comercial e industrial; elaborar diretrizes para a política nacional de proteção de dados pessoais; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento á legislação; apreciar petições de titular contra controlador após comprovada pelo titular a apresentação da reclamação; promover na população o conhecimento das normas e das políticas públicas sobre a proteção de dados pessoais e das medidas de segurança; promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade" (BRASIL, 2018. Artigo 55)

De forma geral, a ANPD fica responsável por garantir o cumprimento da lei, mantendo-se enquanto uma intermediadora dos conflitos entre empresas, pois a ela cabe tanto fiscalizar as práticas de tratamento de dados, como é responsável pelas petições dos titulares de dados contra os agentes de tratamento de dados. Além disso, foram estabelecidas funções educacionais e de pesquisa à ANPD, pois é a partir dela que a população deverá ter conhecimento acerca das políticas públicas de proteção aos dados, e que se promoverá pesquisas relacionadas a proteção de dados. Além da ANPD, que tem responsabilidades fiscalizadoras e regulatórias, a lei apresenta também o Conselho Nacional de Proteção de Dados Pessoais e de Privacidade, que é composto por um representante para cada uma dessas instâncias: Senado Federal; Câmara dos Deputados; Conselho Nacional de Justiça; Conselho Nacional do Ministério Público; Comitê Gestor da internet no Brasil, além de três representantes da sociedade civil, representantes da comunidade científica, dos sindicatos e das empresas. Cabe a este conselho propor diretriz e sugerir ações para a ANPD, além de elaborar relatórios referentes a ações da Política Nacional de Proteção de Dados Pessoais. O conselho também é responsável por elaborar conhecimento e disseminá-lo para a população (BRASIL, 2018. Artigo 58).

Pode-se dizer que, das características fundamentais do capitalismo de vigilância, três foram especialmente atingidas pela LGPD, sendo elas: o acúmulo indeterminado de dados, que é limitado pelos artigo 2º, 6º e 7º, especialmente; o incontrato, também pelo artigo 7º, e a transnacionalidade, pelo capítulo quinto da lei. Algumas características parecem ter sido menos atingidas ou nada alteradas, sendo elas a: Integração das tecnologias de vigilância na sociedade como um todo, o colonialismo de dados e a divisão desigual da aprendizagem[9]. As cidades

[9] Evidencia-se que o colonialismo de dados, enquanto uma forma de colonialidade, possui uma complexidade sociológica e histórica de tal profundidade que dificilmente uma lei ou mesmo um conjunto de leis seria capaz de revertê-la de fato, mas não deixa de ser notório que não há qualquer forma aparente de contestação da lei sobre esse fenômeno.

inteligentes teriam de ser profundamente alteradas para se adequarem à exigência do consentimento, caso as vigilâncias inerentes a elas se legitimassem através do consentimento.

Algumas questões relevantes trazidas pela LGPD não foram ainda bem exploradas, isto é, as formas legais de coleta de dados por parte das empresas a despeito do consentimento, e como a LGPD atinge pequenas empresas que utilizam da coleta de dados. Tais tópicos serão melhor elaborados a seguir.

4.5 Artigo 10º e o problema do legítimo interesse

O artigo 10º da lei afirma:

> Art. 10º O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (BRASIL, 2018, Artigo 10º)

Alguns autores trazem a relevância do legítimo interesse dentro da lei, podendo ser tido como um recurso facilitador às empresas captalizadoras de dados para justificar e legalizar suas operações a despeito do posicionamento dos usuários das redes:

> Se no consentimento, deixava-se poder exacerbado na mão do titular de dados, com um controle total do tratamento de seus dados pessoais, na base legal do legítimo interesse entende-se que o interesse, muitas vezes comercial, do controlador, é legítimo a ponto de afastar a aplicação das outras bases legais (CUNHA, 2021, p.48)

Existe a possibilidade das empresas tratarem dos dados dos usuários de forma legal ainda que não haja um acordo explícito entre eles, no caso, esta possibilidade se justificaria a partir do “legítimo interesse” das empresas sobre a operação de dados. A lei não explicita exatamente o que se pode entender por um legítimo interesse, no entanto, este legítimo interesse é limitado pela lei, que explica em seu décimo artigo:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador; e

> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.
>
> (BRASIL, 2018, artigo 10º)

O artigo trinta e sete complementa este: "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse" (BRASIL, 2018, artigo 37º).

Estas são todas as passagens que a lei traz referente à legalidade do tratamento de dados com base no legítimo interesse. Vários autores sinalizaram como esses dois momentos da lei são de extrema relevância, pois colocam o legítimo interesse como um meio para o uso e coleta de dados dos usuários a despeito de seu consentimento: "não há previsão legal expressa para a oposição ao tratamento de dados pessoais lastreado no legítimo interesse para fins de marketing, um dos setores que certamente mais utilizará essa base legal" (GLITZ, 2019, p.99). Glitz não foi a única autora a trazer a problemática em torno do legítimo interesse. Para Neto (2023), o legítimo interesse é:

> uma maneira preocupantemente fácil de evitar qualquer aparência de controle do usuário. As empresas podem alegar que os dados coletados dos usuários servem à otimização do sistema e melhoramento do serviço para todos, configurando, então, o interesse legítimo previsto no dispositivo acima citado (NETO, 2023, p.138).

O legítimo interesse limita-se a dados não sensíveis e é, ao menos hipoteticamente, conhecido do usuário na medida em que as empresas alertam os cidadãos do uso deste mecanismo ao coletarem seus dados, mas Neto (2023) chama a atenção ao fato de que, uma vez que as empresas possuem esses dados e os algoritmos elaboram funções sobre eles, existe uma profunda imprevisibilidade sobre as conclusões advindas destas operações algorítimias. Para dizer de outra forma, ainda que o legítimo

interesse esteja limitado a quais dados serão capturados a partir dele, as informações advindas das análises desses dados não são:

> Finalmente, e o mais problemático, uma característica muito citada do tratamento de dados é que ela pode dar respostas a perguntas nem mesmo pensadas anteriormente, que não estavam nos termos de consentimento inicial. Assim, o big data desafia a ideia fundamental de Proteção de Dados que é a transparência de processamento. O big data atua como uma "caixa preta"; os dados entram e saem, mas o algoritmo que cria o resultado geralmente é invisível para o usuário e os resultados muitas vezes inescrutáveis. (NETO, 2023, p.143 e 144)

As pesquisas dos dois autores anteriormente citados permitem entender que o legítimo interesse pode ser interpretado como uma forma legal das empresas dispensarem qualquer consentimento dos usuários alegando que o sequestro dos dados é parte fundamental do apoio e promoção de suas atividades, por exemplo, uma empresa focada em compra e venda de produtos alimentícios através da internet pode alegar que não pede consentimento dos usuários para registrar seu histórico de pedidos e traçar um perfil de consumo do usuário porque isto é parte fundamental de suas operações. Neste caso, a empresa não comete nenhuma ilegalidade, à luz da LGPD. Outro exemplo é:

> a sugestão de vídeos similares aos assistidos dentro de uma mesma plataforma. Ora, principalmente com serviços gratuitos, os dados pessoais são utilizados como pagamento, principalmente para a realização de publicidade comportamental. Assim, é um legítimo interesse do controlador que o usuário passe mais tempo dentro da plataforma de vídeos, motivo pelo qual estas plataformas sugerem vídeos de interesse do titular (BIONI, 2021, p.53)

Uma limitação muito abrupta e rigorosa do acúmulo e, consequentemente, da capitalização de dados, de certo faria com que a lei dificilmente fosse aplicável, ou se quer fosse aprovada, o que fez com que os legisladores se preocupassem em colocar, na própria lei, mecanismos para desviar-se das obrigações que ela coloca:

> o que se espera da leitura do legítimo interesse é que ele construa uma estabilização sobre a sua linguagem imprecisa e ao mesmo tempo proporcione o progresso necessário à legislação. Como já mencionado, estamos diante de uma norma que precisa acompanhar tanto as evoluções tecnológicas quanto as evoluções das relações sociais e somente por meio de uma cláusula geral que isso seria possível (GLITZ, 2023, p. 56)

Ou seja, o legítimo interesse surge por uma necessidade da lei "acompanhar as mudanças de seu tempo", portanto, o legítimo interesse precisa ser volúvel para prevenir que a lei freie demais a coleta de dados pelas empresas. O legítimo interesse expressa a tensão entre os interesses das empresas e dos usuários, tensão essa que perpassa toda a LGPD, e que, de certa forma, ela busca conciliar, ora exigindo consentimento, ora estabelecendo fissuras em seu

ordenamento para que isto não signifique prejuízos demais ao meio empresarial voltado ao mercado de dados.

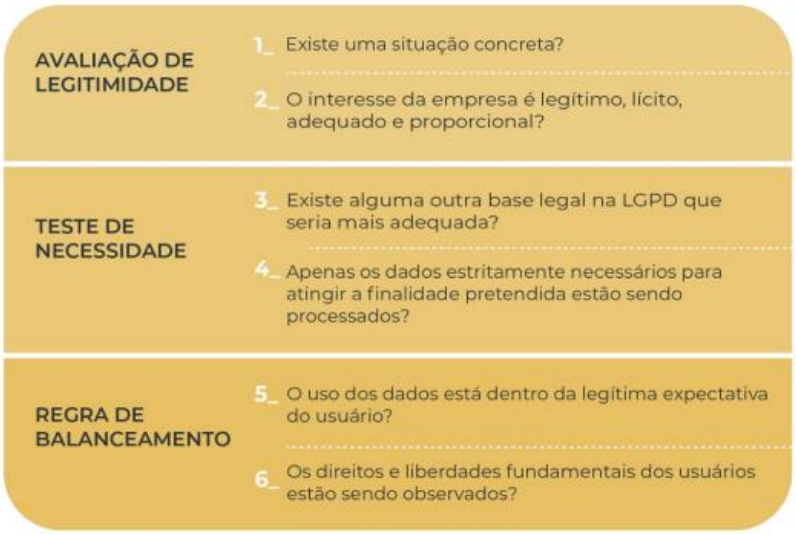
Importante destacar também que a LGPD, em seu artigo 11º, veda a coleta de dados pessoais sensíveis sem o consentimento do titular, independentemente desses dados serem ou não objeto de interesse legítimo das empresas (BRASIL, 2018, Artigo 11). Em outras palavras, é vedada a autoridade das empresas de tratar esses dados para fins econômicos simplesmente. Retoma-se o que a lei entende por dado pessoal sensível:

> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018, artigo 5º)

Além disso, o artigo 7º, antes apresentado, evidencia que o legítimo interesse não pode se sobrepor aos direitos fundamentais dos cidadãos, sendo assim mais um limite para o uso do legítimo interesse.

Para além destes fatores, seria fundamental que as empresas buscassem uma justificativa para o tratamento que não se desse por via do legítimo interesse, além de que os dados em si devem ser bastante restritos ao que é fundamental ao tratamento de dados. A figura abaixo trata destas prerrogativas para o legítimo interesse:

Figura 2



Fonte: RAMOS, 2019.

Parece evidente que, de certa forma, o legítimo interesse funciona, com certas barreiras, como um legitimador para o controle de dados um tanto mais sensível que a por contrato, isto porque não existe uma explícita prévia aceitação do usuário sobre este tratamento, ainda que a lei preveja que ele seja avisado sobre a operação em si. É evidente também que a lei se preocupou em estabelecer certos limites para o uso do legítimo interesse, mas não deixa de ser um mecanismo potente para que as empresas ignorem o consentimento dos usuários. A consequência deste mecanismo é que as empresas, mesmo que não consigam a aprovação de suas operações por parte dos usuários, conseguirão executá-las legalmente, ou seja, existe nisto um relativo desequilíbrio de poder entre cidadãos e empresas de tecnologia: se possível, as empresas terão o aceite em contrato para suas operações, que colocam como indispensável para que se utiliza seus produtos, se não for possível, ainda assim conseguirão tratar os dados, por legítimo interesse (GLITZ, 2019; NETO, 2023). Fica evidente o desequilíbrio de poder, pois não há, em contrapartida, a possibilidade do legítimo interesse do usuário de não ter seus dados tratados ainda que aceite o contrato, mas existe a possibilidade legal da empresa tratar os dados, ainda que não haja aceite para isso.

4.6 A anonimização de dados

O artigo 12º da lei em questão afirma:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais.

Os dados anonimizados, portanto, não são contemplados por essa lei, uma vez que se entende que tais dados não podem ser considerados pessoais, na medida em que não há um vínculo explícito entre eles e seus detentores originais, isto é, as pessoas dos quais eles tratam. E se não há essa explícita relação, o que se tem é a descaracterização do dado enquanto pessoal. Como observa a autora:

> uma vez desvinculados de seu titular, seria aparentemente desafiador defender a proteção jurídica voltada aos direitos de personalidade para esses dados. Afinal de contas, de quem seria a personalidade a ser protegida se, pelo conceito legal, o dado anonimizado é justamente aquele desvinculado de seu titular? (CARVALHO, 2024, p.36)

A mesma autora nos lembra que a LGPD é uma lei de proteção à personalidade, e que, se nenhuma personalidade está em risco diante dos tratamentos, ela tecnicamente não possui aplicabilidade. Os legisladores ainda se atentam ao fato de que, caso a anonimização seja revertida, ou potencialmente revertida com esforços razoáveis, este dado continua sendo pessoal, e pode vir a ferir a personalidade, de forma que deve ter todo seu tratamento fundamentado pela LGPD. Importante observar que a lei não diz o que são esforços razoáveis de reversão da anonimização, mas define o que são dados anonimizados: “III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (BRASIL, 2018, Artigo 5º). Mais uma vez, há uma falta de definição, pois a lei não traz o que são meios razoáveis e disponíveis na ocasião de seu tratamento, deixando uma abertura para múltiplas interpretações.

Esta não preocupação com a defesa da personalidade diante da anonimização dos dados parece infundada uma vez que nenhuma anonimização é perfeita, isto é, nenhum dado está absolutamente desvinculado de qualquer pessoa ou comunidade, e, se assim o fosse, esses dados perderiam muito de seu valor de troca, já que não seriam meios confiáveis e razoáveis para a

manutenção do imperativo de predileção, isto é, o imperativo do capitalismo de vigilância de sempre buscar antecipar e modular comportamentos humanos com fins mercadológicos. De forma resumida: o dado pode ser útil ou perfeitamente anônimo, mas nunca os dois (CARVALHO, 2024, p.54).

Além disso, se o dado nunca está absolutamente desvinculado, nunca "paira suspenso no ar", é importante observarmos que muitas vezes eles podem tratar das personalidades de coletividades, ou seja, por mais que o dado talvez não permita dizer sobre um, pode dizer sobre muitos:

> temos cada vez mais clareza na percepção de que os dados pessoais não envolvem apenas um indivíduo, mas por vezes atribuem características por inferência a toda uma coletividade. Nesse sentido, o dado anônimo, de forma mais abstrata do que o pessoal, fornece informações verídicas, que podem pertencer, se não a um indivíduo específico, a uma categoria analisada (CARVALHO, 2024, p.37)

Carvalho (2024) chama a atenção para o fato de que, se partimos do pressuposto de que as personalidades não se limitam ao escopo individual, mas assumem conotações coletivas, isto é, dizem sobre uma ou mais sociedades, anonimizar o indivíduo não diz sobre anonimizar a coletividade, e, se é assim, por mais que o indivíduo consinta em compartilhar seus dados às empresas de tecnologia, não será apenas os seus dados que estarão sendo cedidos, mas o do coletivo ao qual ele pertence. A LGPD, no entanto, ao focar no direito do consentimento do cidadão especificamente, não parece ter em foco essa noção mais ampla em torno da personalidade trazida pela autora. O que se tem, na prática, portanto, é que as coletividades estão abandonadas no momento de mediação para a permissão do tratamento de dados pelas empresas. Por mais que as suas operações atinjam diretamente sociedades inteiras, volta-se à figura do indivíduo impotente no momento de legitimar tais operações.

Se a anonimização de dados parece uma medida tão frágil na defesa das personalidades coletivas e mesmo individuais, dada sua sempre possível reversão, é importante que se reflita sobre o que a fundamenta em uma lei voltada à proteção dos cidadãos. Pode-se estipular que, assim como o legítimo interesse, a anonimização de dados surge como uma forma de garantir plena operação das empresas capitalizadoras de dados, apesar de sua existência, isto é, estes mecanismos acabam por ser convidativos para que as empresas, ao invés de buscarem os consentimentos de seus clientes, apenas anonimizem seus dados, ou então se sustentem pelo legítimo interesse.

> Nesse contexto, a anonimização parece surgir como uma bala de prata, uma vez que promove uma alternativa às restrições legais, mantendo o dado anonimizado ao livre dispor dos gestores de banco de dados, já que não são considerados dados pessoais (art. 12 da LGPD). A confidencialidade assegurada na própria estrutura do dado traria a liberdade de manutenção das bases Big Data, além da continuidade de seu crescimento e aprimoramento dos algoritmos de tratamento, sem restrições (CARVALHO, 2024, p.49)

Ambos os mecanismos, em especial a anonimização de dados, exigirão um esforço razoável das empresas, mas de forma nenhuma se tornará um obstáculo intransponível para suas operações voltadas à capitalização de dados, se consideradas as grandes empresas, que possuem mais recurso para se adaptar às exigências legais. A próxima seçãose ocupará de tratar dos reflexos da LGPD na operação das pequenas e micro empresas, que, muitas vezes, precisam, tanto quanto as grandes, se adaptarem às imposições legais, no entanto, com muito menos recursos disponíveis.

4.7. A LGPD e as pequenas e micro empresas

Até este momento da pesquisa houve um expressivo foco sobre as big techs, mas essas são a minoria das empresas atingidas pela LGPD. De fato, a Lei Geral de Proteção de Dados diz respeito a todas as empresas as quais usam, de alguma forma, do acúmulo de dados de seus clientes para fins econômicos (BRASIL, 2018, Artigo 1º e 3º). O que significa dizer que existe um amplo grupoempresarial que coleta dados de seus clientes e precisa se adaptar à LGPD, mas com expressiva maior dificuldade, visto que não possue os recursos disponíveis de empresas como a Alphabet e semelhantes para a promoção das mudanças exigidas.

> não resta dúvida de que a questão dos custos de compliance e adequação apresenta um impacto maior para os small business, uma vez que o capital disponível para investimentos em uma empresa é limitado. Para arcar com os custos citados, é habitualmente necessário que a empresa faça um remanejamento de verbas que seriam utilizadas em outras frentes, como o desenvolvimento de produtos e a contratação de pessoal (SILVA, 2024, p.123)

Os altos custo de adequação à LGPD, que afetam especialmente as pequenas e micro empresas[10], fazem com que exista uma expressiva desigualdade sobre como ela atinge as empresas como um todo, de forma que estas empresas mais vulneráveis poderão ter, muitas vezes, que reduzir seus recursos para contratação, ou até mesmo impedir uma empresa de atuar com acúmulo de dados de qualquer forma (SILVA, 2024). Corrobora para estas afirmações a

[10] isto é, empresas com receita bruta anual inferior a 4.8 milhões de reais ao ano (SEBRAE, 2023)

pesquisa publicada pela empresa Daryus, que afirma que até 2023, 83% das empresas consideravam relevante a proteção de dados, mas apenas 20% de fato estavam totalmente adequadas à LGPD (Daryus, 2023). Isto expressa que, por mais que pequenas empresas percebam a real importância de prezar pela proteção dos dados de seus clientes, certamente possuem dificuldades em estar plenamente adequadas às exigências da LGPD.

A ANPD, considerando estas dificuldades, estabeleceu duas medidas para facilitar a adequação destas empresas, são elas: dispensar as pequenas empresas de possuir um encarregado pelo tratamento de dados e a criação de um manual de adequação voltado às pequenas e micro empresas. Tal manual, intitulado “SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE”, possui vinte e uma páginas ao todo e é focado em apresentar boas práticas para a proteção de dados, como treinar os funcionários em proteger os dados e prevenir possíveis ataques hackers e exigir medidas de proteção da informação, caso o serviço de dados da empresa seja terceirizado, além de incentivar as empresas a coletar dados apenas estritamente necessários às suas operações (BRASIL, 2021).

Percebe-se também que estas empresas encontrarão maior dificuldade caso busquem se evadir do consentimento dos titulares de dados, em especial se optarem pela anonimização de dados, isto porque o custo para uma anonimização segura e eficiente dos dados é elevado, além disso, como foi posto anteriormente, anonimizar demasiadamente os dados reduz seu valor: “De forma semelhante ao que ocorre com a criptografia, a anonimização perfeita, se possível, seria extremamente custosa, além de levar a uma perda total ou muito significativa da utilidade do dado” (CARVALHO, 2021, p.52). Conclui-se que a LGPD atinge de forma diversa as pequenas empresas e as grandes empresas de tecnologia, de forma que as pequenas empresas são amplamente mais prejudicadas, ainda que hajam previsões legais de amparo a tais empresas. Posta esta relação desigual entre a LGPD e as empresas, é necessário voltar-se a relação entre esta lei e os cidadãos.

5. A LGPD na relação entre empresas e cidadãos

Os mecanismos que a lei apresenta para a preservação do indivíduo em relação às empresas de tecnologia são voltados à condição contratual estabelecida entre empresa e usuário. Por meio dela, cabe ao usuário aceitar ou não as condições para o uso dos serviços apresentados por determinada empresa, além de que a lei exige transparência quanto aos dados coletados e a que funções estão sendo utilizados, além de estabelecer a criação de um órgão público responsável pela fiscalização do cumprimento das normas por parte das empresas de tecnologia. Com a lei, portanto, impede-se uma coleta de dados indesejada por parte de seus titulares e garante-se que tais titulares tenham acesso a como seus dados estão sendo geridos pelas empresas. Não há estabelecido na lei formas de enfrentamento a vários dos problemas listados anteriormente, os quais exigem outras medidas do Estado. Apesar disso, a LGPD não deixa de se estabelecer como uma importante ferramenta de proteção dos cidadãos, pelas vias contratuais, pois impede que tais empresas utilizem-se de meios para captar dados de pessoas a despeito de sua autorização. Considerando que a lei tem por princípios proteger a privacidade e a autodeterminação informativa, deve-se questionar se ela cumpre com estes princípios, ou se apenas os condiciona a uma relação contratual com os operadores de dados.

5.1 As funções da LGPD

Ficou evidente, pela exposição anterior, que o consentimento do titular de dados é fundamental para a legalidade da coleta e circulação de dados, que deve se dar de forma voluntária e evidente, a não ser nos casos de tratamento sustentados pelo legítimo interesse ou anonimização. O que sustenta esta imposição da lei como forma de regular a relação entre empresas e usuários é a ideia de que cabe aos cidadãos terem poder de determinação e controle sobre a circulação de informações sobre cada um, controle o qual se encontrava enfraquecido diante de uma lógica econômica que priorizava o compartilhamento da vida mesmo em suas dimensões menos públicas. O enfraquecimento do poder decisório sobre a circulação e comercialização de informações pessoais significa uma perda de liberdade dos cidadãos em ter sua posição considerada no âmbito da circulação de dados. Neste sentido a lei reconhece este enfraquecimento e restitui o poder ao titular de dados de impor-se, em alguma medida, nesta relação comercial (SILVA, 2019). Para Bioni e Monteiro (2019), a LGPD garante a legalidade de uma relação econômica de troca em que os usuários apresentam seus dados às empresas em troca de serviços ofertados por ela:

> Os usuários poderão "levar" consigo seus dados pessoais ao trocar uma aplicação na Internet por outra – ou qualquer outro tipo de serviço que se valha do tratamento de dados pessoais –, devendo, inclusive, a antiga aplicação fornecer os meios adequados para operacionalizar tal transmissão de dados, preferencialmente através de protocolos interoperáveis" (BIONI, Bruno; MONTEIRO, Renato. 2019, p.245)

Além disso, as empresas de tecnologia poderão interpretar a LGPD como mecanismo para a proteção de seus interesses no Brasil, pois a legislação torna previsível as relações que as empresas terão com o Estado brasileiro e os usuários, garantindo assim mais estabilidade para suas operações em relação aos brasileiros. Desta forma, os autores não entendem esta lei como um dispositivo impeditivo para as operações de capitalização de dados e para seu desenvolvimento no Brasil, pelo contrário, ela pode ser a base legal para que as empresas de tecnologia desenvolvam suas operações em território nacional.

5.2 A LGPD e a exploração Big Techs/cidadãos

Ainda sobre as formas pelas quais a LGPD atua em relação ao mercado global de dados, para Fornasier e Knebel:

> A LGPD pode ser considerada um suporte jurídico para a acumulação capitalista na era informacional, possibilitando a condição de um titular de direitos relativos aos dados que pode negociar os seus dados com as empresas capazes de lidar com o contexto do *Big Data* e extrair desses dados comportamentos a serem vendidos em um mercado de dados que vende previsões de consumo e de vida cotidiana (FORNASIER; KNEBEL. 2021, p.1003)

Para estes autores, a lei não apresenta propostas realmente efetivas para a proteção dos cidadãos, mas sim para estabelecer sustentação para extração de dados no Brasil, pois, reduzindo a relação entre empresas de tecnologia e usuários em uma relação contratual, se está estabelecendo o poder destas empresas em firmar contratos comerciais com os brasileiros que priorizem mais os interesses das empresas, pois, pela lei, contanto que o contrato seja aceito de forma consciente e não viciosa, ele é legítimo. Com isso, a lei não apenas não limitaria as relações comercias das empresas de dados com a população brasileira, como pode gerar segurança jurídica para que elas desenvolvam mais relações comerciais de dados:

> A LGPD tende a permitir a criação de maiores condições para implementação de um mercado de dados no Brasil, sendo o consentimento do titular o instrumento de regulação e legitimidade que a lei entrega a esse novo mercado, tornando a exploração de dados nada além de uma contratação. (FORNASIER; KNEBEL. 2021, p.1006)

Os autores observam como a mercantilização dos dados faz com que a "digitalização da vida", isto é, a reestruturação de diversas atividades diárias ao meio digitalizado, leva à privação destas mesmas atividades, pois são experiências de vida que são traduzidas em mercadorias

para lucro de um terceiro. Mas como este processo se dá de forma “invisível”, ainda que esteja previsto em contrato, existe uma aceitabilidade maior, pois o que está posto objetivamente são as ferramentas e possibilidades trazidas pelo poder da digitalização da vida. E é neste sentido que os autores concordam com Zuboff ao afirmar que:

> A assimetria informacional é o fator estrutural determinante dessa economia dos dados, justamente pela profunda desigualdade entre a capacidade de gerir e processar dados entre os usuários, titular dos dados pessoais, e quem os controla, as Big Techs” (FORNASIER; KNEBEL, 2021, p.1012)

Essa assimetria informacional é também o que reduz os usuários a meros contratantes, pois seus desconhecimentos em torno dos meios digitais, da captura, acúmulo e capitalização de dados não permitem que tenham capacidade de estabelecer uma crítica às tecnologias de vigilância, que acabam por ser lidas (e se apresentam) como meros instrumentos para facilitar tarefas do dia a dia. A assimetria informacional se traduz então em assimetria de poder, pois as grandes corporações dominam as ferramentas digitais as quais criaram e distribuíram, e esta assimetria de poder não aparenta ser reduzida ou revertida a partir da LGPD. Na verdade, é a própria aceitação do contrato do usuário, em sua impotência, que mantém a legalidade das operações de capitalização de dados. Como coloca a autora:

> com o desenvolvimento da tecnologia, houve o aumento da hipossuficiência intelectual e da vulnerabilidade dos sujeitos que estão à mercê de seus aparelhos e conexões, visto que os dispositivos estão em um patamar mais alto do que os cidadãos podem alcançar, tornando-se agentes de vigilância (TROMBETA, 2022, p.39)

Para Fornasier e Knebel (2021), a LGPD não apenas não protege quem se propõe a proteger, isto é, os usuários de aparelhos de captura de dados, mas estabelece condições para que a dominação das grandes empresas de tecnologia em relação aos usuários se concretize de forma legal e contratual, a despeito da impotência estabelecida a partir da desinformação em relação à capitalização de dados. Neste sentido, é importante relembrar que a lei estabelece que é preciso fomentar estudos referentes à capitalização de dados e que a população deve tomar conhecimento das formas operacionais as quais as empresas de tecnologia utilizam, através de campanhas informativas promovidas pela ANPD. Corrobora para esta conclusão uma pesquisa publicada em 2019 pelo Serasa que, a partir da entrevista de 1.564 brasileiros de todas as macrorregiões, afirma que 75% da população brasileira desconhece ou conhece pouco sobre a LGPD, além disso, 60% dos brasileiros consideram a confiabilidade da marca da empresa, bem como o seu histórico com ela, no momento de decidir sobre o compartilhamento de seus dados (Serasa Experian, 2019). Conhecer mais sobre a LGPD e sobre as operações das Big Techs certamente seria útil ao debate público sobre as melhores formas de regulá-las, pois é a partir

do conhecimento das adversidades levantadas pelo cenário tecnológico atual que se pode elaborar as melhores políticas públicas em torno do assunto. Caso contrário, a discussão se torna muito distante da sociedade, pois, apesar das tecnologias de vigilância estarem disseminadas, a discussão sobre seus efeitos não teve a mesma pulverização.

Outro ponto da LGPD que deve ser analisado é seu caráter extraterritorial, isto é, ela não se aplica apenas aos limites do território brasileiro, mas sim a qualquer empresa que trate dados de pessoas brasileiras, de forma independente de onde estejam. Esta definição da lei é uma forma de lidar com a problemática levantada sobre o sentido transnacional do mercado global de dados, desafio este que é respondido pelo caráter também transnacional da lei. Apesar desta colocação parecer singela, é bastante significativa , pois estabelece o poder do Estado brasileiro em estabelecer normas de conduta para além de seu território, assumindo que a problemática apresentada pela lei não se atém aos limites territoriais do Brasil. Evidente que tal colocação da lei também estabelece a pressuposição de que o Brasil, enquanto Estado nação, terá capacidades práticas de fazer com que as determinações que trazem a lei se realizem para além dele, o que faz necessário algum nível de cooperação internacional. Questões públicas de caráter transnacional exigem tal cooperação, mesmo para estabelecer poder para lidar com as empresas que já assumem este caráter fluído entre territórios.

Importante também voltar-se à forma com a qual a lei trata as relações entre empresas e cidadãos. A condição contratual estabelecida entre cidadãos e Big Techs pela LGPD remete ao próprio desenvolvimento do mercado e do Estado, em que se assumem entre cidadãos diversos contratos como forma de estabelecer previsibilidade nas relações e para garantir que estas relações se sustentem, entre outros motivos. É o contrato que legitimará as relações de poder, estabelecendo a elas caráter legal frente aos Estados. Como a pesquisa apresentou até aqui, as relações de poder estabelecidas entre usuários, que são os cidadãos, com as Big Techs, são multifacetadas e complexas, tanto pela condição de dependência crescente que os cidadãos desenvolvem em relação às Big Techs, quanto pelas consequências sociais nas quais estas formas de poder se traduzem, influenciando tendências políticas, decisões e interesses dos mais diversos tipos. Esta condição de dominação e poder parece ser consideravelmente ignorada pela política pública em sua proposta de relação entre as partes, ainda que reconheça em suas intenções a necessidade de proteger os interesses dos cidadãos.

Importante notar que a LGPD não traz uma discussão aprofundada sobre a desigualdade distributiva dos recursos financeiros advindos da exploração de dados nacionais. Em outras

palavras, o acúmulo de capital para além dos limites nacionais a partir de dados brasileiros não é tratado pela lei, apesar de os princípios da LGPD estarem voltados à proteção da intimidade dos indivíduos, e não às desigualdades econômicas postas no cenário do mercado de dados. Parece importante que a legislação acompanhe a já existente discussão sobre este tema, mesmo porque a extração de dados nacionais para a elaboração de lucros extranacionais é uma das características do capitalismo de vigilância que sustenta a leitura das relações neste mercado como colonialistas. Como existe um empenho dos legisladores em defender a autodeterminação dos usuários em aceitar ou não os contratos impostos pelas grandes empresas, não há um olhar atento sobre como essa autodeterminação de fato opera, a saber, como promotora de uma desigualdade econômica, para além da desigualdade de poder.

6. Considerações finais

Esta pesquisa teve como objetivo, desde seu princípio, investigar a relação entre a LGPD e o fenômeno do capitalismo de vigilância e, a partir dela, foi possível entender essa forma de capitalização e as respostas do Estado brasileiro às questões que ela levanta. É fato que esta pesquisa está limitada à própria forma de definir os objetos estudados a partir das obras referenciadas, e que, certamente, outras obras com perspectivas diversas permitiriam desenvolvimentos e conclusões diferentes dos aqui apresentados. A LGPD tem em seu texto caráter normativo que, como se espera de uma lei, busca ser clara sobre o que se quer regular e como pretende fazê-lo, mas, nem por ser lei deixa de ser isento de múltiplas interpretações e leituras sobre seu real impacto na sociedade brasileira.

Na verdade, toda a lei estabelece relações com a sociedade na qual é construída, tanto antes de sua formação quanto posteriormente, sendo ela mesma uma busca por garantir direitos estabelecidos desde a formação da Constituição de 1988. Como reza a Carta, o Estado é obrigado a proteger a personalidade do indivíduo contra ataques quaisquer, de forma que qualquer lei que se oponha a esta interpretação é inconstitucional (FARIAS, 2020). A relação entre os objetos da pesquisa, isto é, o capitalismo de vigilância e a LGPD, pôde ser entendida a partir das limitações que as normas da lei impõem ao fenômeno em questão, assim como os termos nos quais a lei legitima a capitalização de dados e garante legalidade, pois, como já se explicitou, a LGPD não ilegaliza o capitalismo de vigilância, mas estabelece parâmetros para que ele possa existir legalmente.

O capitalismo de vigilância é um tema consideravelmente recente, de forma que os textos que mais se dedicam a tratar deste assunto surgem no fim do século XX, mas que desde que surgiu tornou-se foco de discussão nas várias áreas das ciências humanas, pois ele envolve várias esferas da sociedade, e não se limita a um fenômeno econômico, como esta e outros pesquisas apresentam, mas estende-se a organização das cidades, das eleições, da própria forma de lidar com os aparelhos de vigilância, entre outras questões envolvidas. Com isso, pode-se dizer que o capitalismo de vigilância deverá ser amplamente estudado por todas as ciências que se voltam à forma com a qual as sociedades se organizam.

Evidenciou-se na pesquisa que a possibilidade do acúmulo ilimitado ou quase ilimitado de dados é fundamental ao capitalismo de vigilância, pois é por meio dele que esse tipo de capitalismo emergiu. A LGPD é instituída justamente para regular o acúmulo de dados, ainda que a lei não estabeleça limites quantitativos, e sim limites qualitativos, o que éum avanço no

que diz respeito aos direitos dos usuários em relação às empresas com as quais estabelecem relações para cumprir suas tarefas diárias. Neste sentido, é preciso retomar a ideia de incontrato antes apresentada. Estabelecer o direito dos cidadãos em renunciar do contrato estabelecido entre eles e as empresas depois de já tê-lo firmado é uma resposta direta a este fenômeno. É fato que a imposição do contrato segue apesar da lei, mas ela não deixa de levantar uma possibilidade legal reativa a este fenômeno.

A transnacionalidade do capitalismo de vigilância é outro fator fundamental para pensa-lo cientificamente. Os problemas advindos dessa modalidade de capitalismo exigirão um nível de colaboração entre nações com fins de solucioná-losr Além disso, a relação das empresas privadas com o poder público, de forma ampla, precisa assumir uma postura que permita aos Estados garantirem os direitos dos cidadãos, e não ficarem impotentes diante de injustiças que venham a ser cometidas contra eles. Como tentamos demonstrar, o capitalismo de vigilância abre muitas discussões que têm implicações com as democracias. Dito de outro modo,as tecnologias do século XXI podem ter um potencial ameaçador sobre as democracias modernas, se não forem reguladas pelos Estados Nacionais.

Esta pesquisa soma-se a outras que apontam para o potencial das redes sociais, para o bem e para o mal, para a formação de opinião, tomada de decisão e, consequentemente, eleições, e como é preciso, com urgência, pensar em mecanismos para lidar com os desafios que, ainda que relativamente novos, não deixam de trazer diversas consequências problemáticas para a política democrática.

O encantamento com a nova revolução tecnológica de fins do século XX deve abrir espaço para as críticas pelo mal uso dessas, desde então, e com maior visibilidade nas primeiras décadas do século XXI. É preciso assumir uma postura compreensiva, ao mesmo tempo que crítica, sobre as tecnologias, não para renunciá-las, mas para transformá-las e estabelecê-las como fortes instrumentos na busca por garantias dos direitos diversos e para o exercício da democracia, e não mecanismos maléficos em nome de uma forma inovadora de geração de lucro. Neste sentido, é importante voltar-se aos agentes detentores dos lucros providos pela capitalização extensiva dos dados, isto é, as Big Techs, que, apesar de serem majoritariamente empresas com sede fora dos limites nacionais, possuem imenso poder econômico e político sobre diversos países, inclusive o Brasil.

Se considerarmos que as modulações comportamentais causadas pelas Big Techs são uma violação às liberdades individuais, a preocupação recai sobre as regulações de cada país.

No caso do Brasil, essas violações não são, ao menos expressivamente, eliminadas pelas regulações da LGPD, pois o controle sobre o conteúdo exposto para cada um ainda é inteiramente das grandes empresas de tecnologia e suas ferramentas de manutenção e seleção de conteúdos, de forma que podem, e são, usadas com fins em estabelecer vantagens econômicas e políticas em diversos países do mundo.

Esta sobreposição das grandes empresas de tecnologia sobre a vida dos cidadãos fere a compreensão de liberdade desenvolvida por autores como John Stuart Mill, John Locke, Rousseau, e outros autores que defenderam a liberdade como parte fundamental da vida em sociedade e democrática. Ocorre que, para tais autores, a liberdade deve ser limitada a não causar dano a terceiros, deve vir acompanhada, nos momentos de decisão, da busca pelo bem comum, a partir da consideração sobre o outro, e tal liberdade deve ser preservada pelo Estado, que não deve simplesmente vigiar pelo bem dos mercados, mas pela vida e a liberdade de todos os cidadãos (MILL, 2011; ROUSSEAU, 2018; LOCKE, 2020). Restringir a noção de liberdade aos fins individuais deturpa a liberdade desenvolvida por esses e outros autores, e fere os sistemas democráticos, pois individualiza os cidadãos de tal forma que o senso de coletivo se vê comprometido. Além disso, potencializa os grandes agentes do mercado em sua busca por lucro, o que leva a esta fragilidade do cidadão sobre as grandes empresas, no caso tratado nesta pesquisa, as Big Techs. Se os Estados não se mobilizam ativamente na defesa dos cidadãos, eles tendem a ser cada vez menos autônomos, menos políticos, menos cidadãos, e mais consumidores e usuários, mais sujeitados aos interesses das grandes empresas.

Entende-se que existe uma vulnerabilidade dos cidadãos nos países nos quais se dão as operações das grandes empresas de tecnologia, que se impõem sem limites bem estabelecidos se não pelas legislações. Desta forma, percebe-se que é fundamental que tais empresas estejam devidamente reguladas pelas autoridades públicas, de forma a cercear os problemas advindos da mal conduta exercida pelas Big Techs em sua busca por mais lucro a despeito das diversas consequências sociais e políticas, as quais esta pesquisa mostrou. Para que isto se concretize, é preciso assumir que as relações de colonialidade persistem no mercado global de dados, pois não se pode entender ou lidar com o capitalismo de vigilância sem assumir as desigualdades historicamente construídas entre os países envolvidos nele. Também é fundamental que se entenda os cidadãos não como meros consumidores, mas como pessoas de direito, que devem ser respeitadas a despeito das relações econômicas. Para dizer de outra forma: não são os direitos fundamentais ao humano que devem ser abdicados diante de um cenário econômico lucrativo, mas os lucros que devem invariavelmente respeitar a integridade humana de cada

pessoa, pois, de outra forma, a pessoa será cada vez mais reduzida a um consumidor ou a uma mercadoria, e a sociedade reduzida a um mercado, seja ele de dados ou não.

O conjunto de autores apresentados permite perceber a estreita relação entre o capitalismo de vigilância e o cenário neoliberal que se desenvolveu nas últimas décadas, e que ocasionou um maravilhamento quanto a potência que os meios digitais representavam para os defensores de amplas liberdades individuais. No entanto, é preciso estar atento aos diversos problemas sociais que podem emergir a partir da capitalização de dados, e quais as possíveis alternativas que o poder público possui para lidar com tais problemas, em que "resolver os problemas" não signifique abolir os novos meios tecnológicos dispersos na sociedade, mas sim pensar em formas de garantir que estes novos meios não signifiquem uma ameaça política para os cidadãos ou para os sistemas democráticos ao redor do mundo:

> A tecnologia, todavia, não deve ser um problema, mas sua presença deve ser construída a partir do diálogo, da intersubjetividade, a fim de que a técnica não venha representar uma perda na identidade pessoal. De igual forma, a privacidade não é um obstáculo, antes se apresenta como a via pela qual as inovações científicas e tecnológicas podem legitimamente entrar em nossa sociedade e em nossas vidas (BAIÃO.; GONÇALVES, 2014, p.15).

Importante destacar também que, para que as tecnologias do século XXI não se tornem verdadeiramente um problema, é preciso que se desenvolva uma cultura em favor da proteção de dados (LUGATI; ALMEIDA, 2022), isto é, é preciso que haja um entendimento público em torno das problemáticas levantadas pelo ambiente digital, e que tal entendimento faça entender a relevância de se debater formas justas e corretas de se lidar com os meios digitais. Sem isto, corre-se o risco de que o cenário político-tecnológico aqui trabalhado seja lidado de forma acrítica, e a redução dos cidadãos à consumidores e produtores de dados poderá ser ainda mais acentuada. Com fins em evitar este cenário é que se torna relevante o olhar crítico comum sobre o acúmulo de dados, o mercado de dados, as tecnologias sequestradoras de dados, etc. As complexidades sociológicas e históricas postas e expressas no capitalismo de vigilância apenas poderão ser amplamente compreendidas se houver um planejamento educacional voltada aos temas aqui trabalhados, pois, considerando a relevância que as tecnologias de vigilância assumiram, é pertinente que os cidadãos tenham acesso ao pleno conhecimento de suas operações, o que permitirá, inclusive, a elaboração de medidas mais sofisticadas de proteção dos cidadãos. Foi posto que uma das características do capitalismo de vigilância é a desigualmente na aprendizagem, isto é, enquanto um grupo muito específico conhece com relativa profundidade as operações feitas a nível algorítmico e entendem relativamente as

consequências delas, este conhecimento não está disseminado devidamente, é preciso que este conhecimento perca sua exclusividade e se torne amplamente conhecido, o que pode ser feito, por parte do Estado, a partir de políticas públicas, em especial no campo da educação.

Por fim, esta pesquisa permite concluir que, ainda que a LGPD tenha apresentado avanços nas garantias de proteção dos cidadãos em relação aos problemas que os meios tecnológicos podem trazer, como por exemplo as exigências mínimas para que o tratamento de dados ocorra e a possibilidade legal da revogação do consentimento, há ainda muito a se avançar no sentido de garantir uma relação plenamente saudável entre novas tecnologias, sistemas democráticos e cidadãos. Importante considerar também que, tendo em vista que os fundamentos da LGPD são o respeito à privacidade, a autodeterminação informativa e outros fundamentos correlacionados, dificilmente ela bastaria para conter todas as questões levantadas pela ampla capitalização de dados, sendo necessário um esforço legislativo mais amplo, certamente com novas políticas públicas. A pesquisa evidenciou como os meios tecnológicos tratados aqui se desenvolveram com fins lucrativos, e não democráticos, isso não significa, porém, que não tenham em si potencial para as democracias, mas quer dizer que a própria estrutura dos meios tecnológicos de diálogo elaborados e disseminados pelas grandes empresas de tecnologia estão fundamentalmente apoiados no lucro, e que fazer deles democráticos envolve regulamentações, políticas públicas, acordos transnacionais entre Estados, e a conscientização dos usuários sobre o cenário que se desenha, além de ser imprescindível o trabalho acadêmico para a elucidação dos desafios postos no século XXI.

REFERÊNCIAS

ARRUDA, Renê. SISTEMAS ALGORÍTMICOS E GOVERNAMENTALIDADE: PERSPECTIVAS DA SOCIEDADE DE CONTROLE E CAPITALISMO DE VIGILÂNCIA. **Anais XII Simpósio Nacional da ABCiber**, [*s. l.*], ano 2019, ed. 12, p. 1-12, 25 jul. 2019. Disponível em: https://www.academia.edu/41366484/SISTEMAS_ALGOR%C3%8DTMICOS_E_GOVERNAMENTALIDADE_PERSPECTIVAS_DA_SOCIEDADE_DE_CONTROLE_E_CAPITALISMO_DE_VIGIL%C3%82NCIA?auto=citations&from=cover_page. Acesso em: 27 jan. 2022 às 08h45.

Byung-Chul Han. No enxame. Rio de Janeiro: Editora Vozes. 2018.

BENTHAM, J. **Uma Introdução aos Princípios da Moral e da Legislação**. In: Os Pensadores v.34. São Paulo: Editora Abril. 1974

BENTHAM, J. **O panóptico**. [s.l.]. Belo Horizonte: Autêntica, 2019.

BAIÃO, K. C. S.; GONÇALVES, K. C. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **civilistica.com**, v. 3, n. 2, p. 1-24, 10 dez. 2014. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/151

BIONI, Bruno; MONTEIRO, Renato Leite. Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia: O impacto econômico de uma lei geral de dados. In: REIA, Jhessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo. Horizonte presente tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito; FGV, p. 232-248, 2019. Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27448/Horizonte%20presente%20-%20tecnologia%20e%20sociedade%20em%20debate.pdf?sequence=1&isAllowed=y.

BIONI, Bruno Ricardo; RIELLI, Mariana Marques. Proteção de dados: contexto, narrativas e elementos fundantes. **São Paulo: BR Bioni Sociedade Individual de Advocacia**, 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: 15 ago. 2018.

BRASIL. SEGURANÇA DA INFORMAÇÃO PARA AGENTES DE TRATAMENTO DE PEQUENO PORTE. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 14 de outubro de 2024.

Bresser-Pereira, Luiz Carlos. **Assalto ao Estado e ao mercado, neoliberalismo e teoria econômica**. Estudos Avançados [online]. 2009, v. 23, n. 66, p. 7-23. Disponível em: https://doi.org/10.1590/S0103-40142009000200002. Acesso em 08 de Outubro de 2021

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., & Fowler, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. Nature, 489(7415), 295–298. Disponível em: https://doi.org/10.1038/nature11421

BARROS BORDIGNON, G. Dispositivos de vigilância como tecnologias de controle no capitalismo de dados: redes sociais e smart cities. **Revista de Morfologia Urbana**, *[S. l.]*, v. 8, n. 2, p. e00157, 2020. DOI: 10.47235/rmu.v8i2.157. Disponível em: http://revistademorfologiaurbana.org/index.php/rmu/article/view/157. Acesso em: 28 jan. 2022.

BROWN, Wendy. Nas ruínas do neoliberalismo: a ascensão da política antidemocrática no ocidente.São Paulo: Politeia, 2019.

BOGARD, W. The simulation of surveillance. Cambridge University Press, 1996.

BRUNO, F. Monitoramento, classificação e controle nos dispositivos de vigilância digital. **Revista FAMECOS**, *[S. l.]*, v. 15, n. 36, p. 10–16, 2008. DOI: 10.15448/1980-3729.2008.36.4410. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/4410. Acesso em: 1 abr. 2023.

BBC. Trump vence, como será o segundo mandato?. Disponível em: https://www.bbc.com/portuguese/articles/c30p8045p13o. Acesso em 10 de janeiro de 2025.

BRAUN, Julia. O que pode estar por trás de decisão da Meta de abandonar checagem independente de fatos. BBC, 8 de janeiro de 2025. Disponível em: https://www.bbc.com/portuguese/articles/c5y4ymrpp43o. Acesso em 10 de janeiro de 2025.

BERNARDES, F.; SOUZA, A. **A plataformização das políticas no Brasil e os seus impactos nas desigualdades**. Disponível em: https://diplomatique.org.br/a-plataformizacao-das-politicas-no-brasil/?fbclid=PAZXh0bgNhZW0CMTEAAabrkUpCIbY-uisaEAlrF4Eg0I1VyONKLlwEewVC5rK2yJZjSBYu-6uV8k8_aem_Ab0QaVtNOh9TlKQo1NYM8on2GekIW6rmeFZ1dW3EitVlk4JQadxW8zzYiPVkbUVhhH1uMqAty3RcLTRkWyNNTDtw. Acesso em: 4 jun. 2024.

COSTA, R. DA .. Sociedade de controle. **São Paulo em Perspectiva**, v. 18, n. São Paulo Perspec., 2004 18(1), p. 161–167, jan. 2004

COSTA, Sérgio. 2006. DESPROVINCIALIZANDO A SOCIOLOGIA – A contribuição pós-colonial. RBCS. ANPOCS, v.21, n. 60, p. 117-183. Disponível em: https://www.scielo.br/j/rbcsoc/a/qvRBnnndFWrz8ZYLKjPzWpS/abstract/?lang=pt. Acesso em 15 de junho de 2024.

CARVALHO NUNES, M. Warburg, Agamben, Deleuze: a imagem e a filosofia da diferença. **MODOS**, v. 4, n. 3, 8 set. 2020. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/mod/article/view/8662709. Acesso em 16 de fevereiro de 2024

CARVALHO, M. A. Capitalismo de vigilância : a privacidade na sociedade da informação. 27 abr. 2019. Disponível em: https://ri.ufs.br/handle/riufs/11425. Acesso em 21 de junho de 2023.

CARVALHO, Fernanda Potiguara. O ser atrás do dado: limites e desafios da anonimização e seus reflexos nos requisitos estabelecidos pela LGPD. 2024. Disponível em: http://www.rlbea.unb.br/jspui/handle/10482/48043. Acesso em 11 de outubro de 2024.

CUNHA, J. B. Legítimo Interesse: a carta (nada) branca da lei geral de proteção de dados (LGPD). Ufsc.br, 2021. Disponível em: https://repositorio.ufsc.br/handle/123456789/228523. Acesso em: 2 de setembro de 2024.

DARYUS. Privacidade e Proteção de Dados Pessoais. 2023. Disponível em: https://materiais.daryus.com.br/workshop-perspectiva-cenario-lgpd-2023?utm_source=imprensa&utm_medium=imprensa&utm_campaign=imprensa_workshopd. Acesso em 18 de outubro de 2024.

GLITZ, Gabriela Pandolfo Coelho et al. Proteção de dados pessoais: uma análise sobre a aplicabilidade do legítimo interesse. 2019.

GAMA, Sophia. Guerra de desinformação: as fake news nas eleições de 2018 — Portal da Câmara Municipal de Curitiba. Disponível em: https://www.curitiba.pr.leg.br/informacao/noticias/guerra-de-desinformacao-as-fake-news-nas-eleicoes-de-2018 . Acesso em 15 de janeiro de 2025.

PADUA, Luciano. **Sorria? Seus dados estão sendo compartilhados**. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-expressao/sorria-dados-compartilhados-29032018. Acesso em: 16 fev. 2024.

TROMBETA, Elena Beatriz Domingues. A eficácia da lei geral de proteção de dados frente ao capitalismo de vigilância.2022. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/30064/1/TCC%20-%20ELENA..%20%283%29.pdf. Acesso em: 16 jun. 2023.

TSE. Eleições 2018: Justiça Eleitoral conclui totalização dos votos do segundo turno. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2018/Outubro/eleicoes-2018-justica-eleitoral-conclui-totalizacao-dos-votos-do-segundo-turno. Acesso em 24 de outubro de 2024.

TRE-PA. 2018 e o impacto das Fake News. Disponível em: https://www.tre-pa.jus.br/comunicacao/noticias/2018/Junho/eleicoes-2018-e-o-impacto-das-fake-news-1. Acesso em: 15 jan. 2025.

FOUCAULT, M. Vigiar e punir : nascimento da prisão. Petropolis: Vozes, 2011.

FORNASIER, M. DE O.; KNEBEL, N.M.P. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. Revista Direito e Práxis, V.12, abril de 2021. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/. Acesso em 16 de junho de 2023.

FARIAS, Thalyta Soares de. Privacidade, monetização de dados pessoais e a LGPD: desafios e impactos da Lei Nº 13.709/2018. 2020. Monografia (Bacharelado em Direito) - Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2020. Disponível

em: https://repositorio.uniceub.br/jspui/handle/prefix/14277 . Acesso em 15 de novembro de 2023.

GILLESPIE, T. A relevância dos algoritmos. **Parágrafo**, v. 6, n. 1, p. 95–121, 29 jun. 2018.

G1. Jair Bolsonaro é eleito presidente com 57,8 milhões de votos. Disponível em: https://g1.globo.com/politica/eleicoes/2018/apuracao/presidente.ghtml. Acesso em 24 de outubro de 2024.

HARVEY, D. **O neoliberalismo : história e implicações**. São Paulo: Loyola, 2008.

IANNI, O.. Globalização: novo paradigma das ciências sociais. Estudos Avançados, v. 8, n. 21, p. 147–163, maio 1994. Disponível em: https://www.scielo.br/j/ea/a/B8N9NgC4F9XkXZjpGqZMFzr/#ModalHowcite. Acesso em 07 de junho de 2024

LUGATI, L. N.; ALMEIDA, J. E. de. A LGPD e a construção de uma cultura de proteção de dados. Revista de Direito, [S. l.], v. 14, n. 01, p. 01–20, 2022. DOI: 10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 5 fev. 2024.

LOCKE, J. **Segundo tratado sobre o governo civil e outros escritos.** Editora Vozes, 2020.

MEIRELES, A. V.. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, v. 27, n. Opin. Publica, 2021 27(1), p. 28–50, jan. 2021

MILL, John. **Sobre a liberdade**. Editora Saraiva, 2011.

MELGAÇO, Lucas. ESPAÇO E VIGILÂNCIA: REFLEXÕES A PARTIR DA GEOGRAFIA NOVA. **3 o Simpósio Internacional LAVITS: Vigilância, Tecnopolíticas, Territórios**, ed. 3, p. 328-341, 13 de maio de 2015. Disponível em: https://medialabufrj.net/download/arquivos/lavits2015-anais/5/5.Resumo103.pdf. Acesso em: 8 fev. 2022.

MISKOLCI, R. Sociologia Digital: notas sobre pesquisa na era da conectividade. **Contemporânea - Revista de Sociologia da UFSCar**, v. 6, n. 2, p. 275–275, 2016.

Martins, Paulo Henrique. Norte e Sul como Referências para uma Ciência Social global: Transdisciplinar, Antiutilitarista e Pós-Colonial. Revista TOMO, núm. 31, 2017, Julho-, pp. 41-89 Universidade Federal de Sergipe Brasil. Disponível em: https://doi.org/10.21669/tomo.v0i0.7649. Acesso em 06 de julho de 2023.

MACHADO, D. F. A modulação algorítmica de comportamento e suas categorias operativas a partir das patentes da Facebook Inc. Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura, v. 22, n. 2, p. 97–111, 24 maio 2020

MOROZOV, E. Big Tech : a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

NETO, Gabriel de Oliveira Cavalcanti. LGPD, CIDADES INTELIGENTES E PRIVACIDADE.

NASCIMENTO, L. F.. A Sociologia Digital: um desafio para o século XXI. Sociologias, v. 18, n. 41, p. 216–241, jan. 2016.

Por que Hillary perdeu a eleição mesmo recebendo mais votos que Trump. **BBC News Brasil**. Disponível em: https://www.bbc.com/portuguese/internacional-37948302. Acesso em 01/04/2023 às 13h23

Portal da Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em 16 de fevereiro de 2024.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais - 2a Edição 2020**. Editora Saraiva, 2020.

Privacidade hackeada. Direção: Karin Amer; Jehane Noujaim. Estados Unidos: Netflix. 2019.

PAULANI, L. M. Neoliberalismo e individualismo. **Economia e Sociedade**, Campinas, SP, v. 8, n. 2, p. 115–127, 2016. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/ecos/article/view/8643138. Acesso em: 4 out. 2021.

PEREIRA, A. E.. Três perspectivas sobre a política externa dos Estados Unidos: poder, dominação e hegemonia. **Revista de Sociologia e Política**, v. 19, n. 39, p. 237–257, jun. 2011

PATEMAN, C. **Participação e Teoria Democratica**. São Paulo: Paz E Terra, 1992.

QUIJANO, A. COLONIALIDADE, PODER, GLOBALIZAÇÃO E DEMOCRACIA. **Revista Novos Rumos**, *[S. l.]*, n. 37, 2022. DOI: 10.36311/0102-5864.17.v0n37.2192. Disponível em: https://revistas.marilia.unesp.br/index.php/novosrumos/article/view/2192. Acesso em: 16 jun. 2023.

RAMOS, Pedro. A REGULAÇÃO DE PROTEÇÃO DE DADOS E SEU IMPACTO PARA A PUBLICIDADE ONLINE: UM GUIA PARA A LGPD. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/07/MP_guia_LGPD.pdf. Acesso em 07 de fevereiro de 2024.

RAMOS, L.; ZAHRAN, G. Da hegemonia ao poder brando: implicações de uma mudança conceitual, pp. 134-160 DA HEGEMONIA AO PODER BRANDO: IMPLICAÇÕES DE UMA MUDANÇA CONCEITUAL. [s.l: s.n.]. Disponível em: <https://biblat.unam.mx/hevila/CENAInternacional/2006/vol8/no1/9.pdf>. Acesso em 18 de junho de 2023.

ROUSSEAU, Jean-Jacques. O Contrato Social. São Paulo: Lafonte. 2018.

SCHIAVI, Iara. As tendências neoliberais e dataficadas da incorporação tecnológica nas cidades. In:Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, p. 148-166. 2021.

Souza, Joyce; Avelino, Rodolfo; Silveira, Sérgio Amadeu da (Org.). A sociedade de controle: manipulação e modulação nas redes digitais. 1. ed. São Paulo: Hedra, 2018

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação; KFOURI, Gustavo. A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA AUTONOMIA PRIVADA EM UM MUNDO CADA VEZ MAIS TECNOLÓGICO. **Revista Juridica**, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581>. Acesso em: 07 abr. 2023.

SILVA, Fernando Mendes Naegele. A geração de efeitos concorrenciais pela LGPD para as microempresas e empresas de pequeno porte. 2024. Disponível em: https://bdtd.ibict.br/vufind/Record/FGV_afb91719c5d6babf95c49285c222bcb2. Acesso em 14 de outubro de 2024.

Silveira, S. A. (2017). GOVERNO DOS ALGORITMOS. *Revista De Políticas Públicas*, *21*(1), 267–282. https://doi.org/10.18764/2178-2865.v21n1p267-281

SIQUEIRA, . N.; CONTIN, . C.; BARUFI, . B.; LEHFELD, . de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . REVISTA ELETRÔNICA PESQUISEDUCA, [S. l.], v. 13, n. 29, p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 1 fev. 2024.

SILVEIRA, S. A. DA. **Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas**. [s.l.] Edições Sesc, 2019.

SENADO FEDERAL. Projeto de Lei do Senado n° 246, de 2018. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133353. Acesso em 15 de janeiro de 2025.

SENADONOTÍCIAS. CCJ analisa criação de órgão para acompanhar mídias sociais Fonte: Agência Senado. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/01/17/ccj-analisa-criacao-de-orgao-para-acompanhar-midias-sociais>. Acesso em: 15 jan. 2025.

AMADEU DA SILVEIRA, S. A noção de modulação e os sistemas algorítmicos. **PAULUS: Revista de Comunicação da FAPCOM**, *[S. l.]*, v. 3, n. 6, 2019. DOI: 10.31657/rcp.v3i6.111. Disponível em: https://fapcom.edu.br/revista/index.php/revista-paulus/article/view/111. Acesso em: 21 fev. 2023.

SILVEIRA, S.A. DA. Inteligência artificial baseada em dados e as operações do capital. **PAULUS: Revista de Comunicação da FAPCOM**, *[S. l.]*, v. 5, n. 10, 2021. DOI: 10.31657/rcp.v5i10.480. Disponível em:

https://fapcom.edu.br/revista/index.php/revista-paulus/article/view/480. Acesso em: 16 jun. 2023.

SILVA, F. C. C. DA; PIRES, T. DA S.; WENDT, L. G. Do colonialismo histórico ao colonialismo de dados: reflexões sobre a relação entre Big Data e o sujeito. **Logeion: Filosofia da Informação**, v. 10, n. 1, p. 75–90, 30 ago. 2023.

The Metaverse and How We'll Build It Together -- Connect 2021. Disponível em: https://www.youtube.com/watch?v=Uvufun6xer8&t=474s. Acesso em: 28 mar. 2023.

ULRICH BECK; SEBASTIÃO NASCIMENTO. **Sociedade de risco : rumo a uma outra modernidade**. São Paulo: Editora 34, 2011.

VIANNA, Fernando. Se os Dados são o Novo Petróleo, Onde Estão os Royalties? O Neoliberalismo na Era do Capitalismo de Vigilância. **Revista Gestão & Conexões**, *[S. l.]*, v. 10, n. 3, p. 123–143, 2021. DOI: 10.47456/regec.2317-5087.2021.10.3.36014.128-147. Disponível em: https://periodicos.ufes.br/ppgadm/article/view/36014. Acesso em: 23 jan. 2024.

VIEJO, Manuel; ALESSI, Gil. **Empresários financiaram disparos em massa pró-Bolsonaro no Whatsapp, diz jornal.** Disponível em: https://brasil.elpais.com/brasil/2019/06/18/politica/1560864965_530788.html. Acesso em 24 de outubro de 2024.

POMPEU, Ana. **TSE mantém propaganda do PT que usa esquema de WhatsApp contra Bolsonaro**. Disponível em: https://www.conjur.com.br/2018-out-23/tse-mantem-campanha-usa-esquema-whatsapp-bolsonaro/. Acesso em 24 de outubro de 2024.

ZUBOFF, Shoshana. A era do capitalismo de Vigilância. Rio de Janeiro: Intrinseca. 1ª edição. Fev. 2021.

WEINMANN, A. DE O.. Dispositivo: um solo para a subjetivação. Psicologia & Sociedade, v. 18, n. 3, p. 16–22, set. 2006.

75% dos consumidores desconhecem ou conhecem pouco sobre a Lei de Proteção de Dados, revela pesquisa inédita da Serasa Experian. Disponível em: <https://www.serasaexperian.com.br/sala-de-imprensa/estudos-e-pesquisas/75-dos-

consumidores-desconhecem-ou-conhecem-pouco-sobre-a-lei-de-protecao-de-dados-revela-pesquisa-inedita-da-serasa-experian/>.