UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE DIREITO

Ramon Romeiro Zanirato

DIREITO E TECNOLOGIA:
O CAPITALISMO DE VIGILÂNCIA E AS FRONTEIRAS DA PROTEÇÃO DE DADOS PESSOAIS

Santa Maria, RS
2023

Ramon Romeiro Zanirato

DIREITO E TECNOLOGIA:
O CAPITALISMO DE VIGILÂNCIA E AS FRONTEIRAS DA PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada ao Curso de Direito da Universidade Federal de Santa Maria, RS, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientadora: Prof.ª Dr.ª Nina Trícia Disconzi Rodrigues Pigatto

Santa Maria, RS
2023

Ramon Romeiro Zanirato

DIREITO E TECNOLOGIA:
O CAPITALISMO DE VIGILÂNCIA E AS FRONTEIRAS DA PROTEÇÃO DE DADOS PESSOAIS

Monografia apresentada ao Curso de Direito, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do título de **Bacharel em Direito**.

Aprovada em 10 de julho de 2023.

_____
Nina Trícia Disconzi Rodrigues Pigatto, Doutorado (UFSM)
Orientadora

_____
Rafael Santos de Oliveira, Doutorado (UFSM)

_____
João Pedro Seefeldt Pessoa, Mestrado (UFSM)

Santa Maria, RS
2023

Para todos aqueles que, em maior ou menor grau,
sonham com um mundo virtual mais seguro.

AGRADECIMENTOS

Toda pesquisa exige um afastamento do nosso lado sentimental. Reservo este espaço para manifestar todas as emoções que tanto me esforcei para manter de fora da parte textual desta monografia.

Em primeiro lugar, este trabalho não teria sido possível sem o apoio e as valiosíssimas orientações da Profe Nina, minha orientadora. Cada um dos encontros de orientação foi de grande esclarecimento, e imprescindível para a conclusão desta monografia. Para além disso, todos os ensinamentos serão levados para toda a minha vida. Por isso, Profe, pela sabedoria e pela paciência, a minha mais sincera gratidão.

Em segundo lugar, este trabalho igualmente não teria sido possível sem o apoio de todas as pessoas que estiveram a minha volta, aguentando todo o estresse, se estressando junto comigo, e espairecendo a mente. A todos vocês, especialmente Carol, Celinha, Gabriel e Mari, o meu muito obrigado.

Em terceiro lugar, mas com a importância do primeiro, a minha família, base de tudo. Sem o apoio para deixar o estado de São Paulo e me aventurar no coração do Rio Grande, muito provavelmente eu não teria chegado até o fim do curso. E, antes disso, a minha gratidão pelo incentivo desde pequeno pelos estudos e pelo amor ao conhecimento. Mamãe, papai e titias, vocês tornaram isso possível.

Por último, mas não menos importante, agradeço a todos os atores que participaram indiretamente deste processo: professores, mestrandos, servidores administrativos, promotores, juízes e assessores que acompanharam o meu trajeto.

Como menção honrosa, agradeço à Universidade Federal de Santa Maria por toda a minha formação. Este trabalho é fruto da educação pública, gratuita e de qualidade, pela qual todos devemos lutar incessantemente e defender com afinco!

Esses invasores do século XXI não pedem permissão; eles avançam, cobrindo a terra devastada com práticas de falsa legitimação. Em vez de editos monárquicos cinicamente transmitidos, eles oferecem acordos de termos de serviço cinicamente transmitidos cujas estipulações são, em igual medida, obscuras e incompreensíveis.

Shoshana Zuboff

RESUMO

DIREITO E TECNOLOGIA: O CAPITALISMO DE VIGILÂNCIA E AS FRONTEIRAS DA PROTEÇÃO DE DADOS PESSOAIS

AUTOR: Ramon Romeiro Zanirato
ORIENTADORA: Nina Trícia Disconzi Rodrigues Pigatto

Com a ascensão das *Big Techs* e desenvolvimento vertiginoso das tecnologias de informação e comunicação (TICs), Shoshana Zuboff teorizou o capitalismo de vigilância. Em uma dinâmica predatória dos dados pessoais do usuário, sua privacidade é violada e sua autodeterminação informativa, corrompida. Nesse cenário, surge o presente trabalho. Busca-se compreender o fenômeno do capitalismo de vigilância, tal qual teorizado por Zuboff, bem como explorar os reflexos nocivos dessa nova dinâmica em relação ao titular dos dados. Após a contextualização do fenômeno e de revisitação de casos emblemáticos da nocividade do sistema, passa-se ao enfrentamento do ordenamento jurídico brasileiro, buscando compreender se o capitalismo de vigilância é recepcionado e regulado, e em que medida é possível falar-se na efetiva proteção dos dados pessoais dos usuários. Foi utilizado o método de abordagem fenomenológico, e o método de procedimento monográfico. A técnica de pesquisa utilizada foi a pesquisa bibliográfica. O principal resultado obtido neste trabalho foi que o ordenamento jurídico brasileiro não recepciona, tampouco regula o capitalismo de vigilância. No entanto, a previsão expressa da proteção de dados pessoais no rol de direitos fundamentais alça o Brasil a um patamar avançado de proteção. Apesar de não se poder falar na efetiva proteção dos dados pessoais, o *status* constitucional representa importante passo rumo à regulação do capitalismo de vigilância, podendo orientar a aplicação da norma em favor do usuário no caso concreto.

Palavras-chave: capitalismo de vigilância; efetividade; proteção de dados pessoais

ABSTRACT

LAW AND TECHNOLOGY: THE AGE OF SURVEILLANCE CAPITALISM AND THE BOUNDARIES OF PERSONAL DATA PROTECTION

AUTHOR: Ramon Romeiro Zanirato
ADVISOR: Nina Trícia Disconzi Rodrigues Pigatto

Due to the rise of big techs and the increasing development of information and communication technologies (ICTs), Shoshana Zuboff has theorized the surveillance capitalism. Through predatory data collection, ICTs violate the user's privacy and right to informational self-determination. This work aims to comprehend the surveillance capitalism, as well as to explore the negative reflexes this new dynamic provokes into the users. After contextualizing the phenomenon and reentering remarkable events, this work faces Brazilian legal system, in order to comprehend whether surveillance capitalism is regulated, and to what extent it is possible to verify effectiveness in the user's data protection. The phenomenological approach method was utilized, as well as the monographic procedure method. The research technique utilized was bibliographic research. The main result obtained is that the surveillance capitalism is not regulated by the Brazilian legal system. However, the express provision of personal data protection as a fundamental right in Brazil's Federal Constitution represents a big step towards the regulation of the surveillance capitalism, although it may not be possible to verify effective protection.

Keywords: effectiveness; personal data protection; surveillance capitalism.

LISTA DE ABREVIATURAS

ADI	Ação Direta de Inconstitucionalidade
ANPD	Autoridade Nacional de Proteção de Dados
CF	Constituição Federal
LGPD	Lei Geral de Proteção de Dados
EC	Emenda Constitucional
MP	Medida Provisória
PEC	Proposta de Emenda à Constituição
STF	Supremo Tribunal Federal
TIC	Tecnologia de Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

"Conexão" talvez seja a palavra do momento. Uma sociedade desconectada é algo impensável atualmente. As tecnologias de informação e comunicação (TICs) integram, compõem, e, em muitos casos, regem setores expressivos da sociedade. Não raras vezes nos pegamos fazendo um pedido por um aplicativo de entregas, ou mesmo por um aplicativo mensageiro. Em outros casos, consultamos um endereço específico em nosso buscador preferido, ou, ainda, fazemos uma busca rápida para verificar a grafia de uma palavra, só por segurança. Pesquisas científicas se tornaram acessíveis graças à disponibilidade de acervos de altíssima qualidade, propiciados justamente em razão da difusão das TICs. Em outro ponto do espectro, organizações sociais somente conseguiram fazer florescer a Primavera graças ao acesso às redes de indignação e esperança.

No entanto, as novas tecnologias trouxeram consigo uma nova dinâmica: carros que podem não dar partida em caso de inadimplemento das parcelas do financiamento; reconhecimento facial como forma de verificar se uma publicidade está sendo bem recebida e o usuário está inclinado a adquirir o produto ofertado; otimização de exibição de conteúdo a fim de instigar o usuário a consumir mais e mais na rede; dentre muitas outras. Como se verá ao longo deste trabalho, o que se chamou Capitalismo de Vigilância – termo cunhado pela pesquisadora Shoshana Zuboff – pressupõe uma interação nociva com o usuário final. Sob tal cenário, justifica-se o presente trabalho diante da premente necessidade de compreender o fenômeno, e, em via de consequência, regulá-lo, para, então, assegurar os melhores serviços e produtos com menores – ou, utopicamente falando, sem – prejuízos ao consumidor.

Cumpre ressaltar que a temática aqui trabalhada pode não se manter atual por muito tempo. Esta área, emergente em relação a muitas outras áreas do Direito, é marcada por intensa volatilidade. Em verdade, viu-se nas novas tecnologias uma dinâmica de "evolução"[1] cada vez mais rápida. O fenômeno experimentado no ano de defesa desta monografia pode se alterar no ano de 2024. A própria legislação pode se expandir (e, como veremos, pode se desdobrar em algo bom, pensando-se no usuário

[1] O uso das aspas é intencional, pois a ideia de evolução tende a implicar uma melhoria constante, sem regressos. Contudo, conforme ao marco teórico deste trabalho, não se pode vislumbrar a evolução – especialmente a das tecnologias de informação e comunicação – como algo constante e sempre para melhor.

final), ou, ainda, revogar a norma enfrentada nestas páginas. De toda sorte, mesmo que se torne totalmente defasado, este trabalho servirá de substrato à atividade historiográfica, o que, novamente, justifica sua existência.

E sob tais condições surge o presente trabalho. Busca-se a compreensão da temática do capitalismo de vigilância, e, na sequência, sua projeção em relação ao ordenamento jurídico brasileiro. Isto é, pretende-se aferir em que medida o ordenamento recepciona e regula esse fenômeno, especialmente em sua matéria mais delicada: a privacidade digital dos usuários das Tecnologias de Informação e Comunicação e a consequente proteção de seus dados. Ao longo deste trabalho, serão enfrentados aspectos da legislação vigente, bem como a jurisprudência do Supremo Tribunal Federal, e qual vem a ser o papel do atual status constitucional da proteção de dados pessoais, introduzida pela Emenda Constitucional (EC) n. 115/22.

O trabalho se divide em dois grandes capítulos, cada um desdobrado em dois subcapítulos. O primeiro capítulo se dedica ao enfrentamento do fenômeno do capitalismo de vigilância. No primeiro subcapítulo, esta monografia busca descrever o surgimento do fenômeno do capitalismo de vigilância, da forma como foi teorizado por Shoshana Zuboff, bem como os reflexos exercidos sobre as tecnologias de informação e comunicação. O segundo subcapítulo, por sua vez, se dedica às nocividades advindas dessa nova lógica de acumulação da informação, com a revisitação de casos emblemáticos ocorridos tanto no Brasil quanto no exterior.

O contexto trazido no primeiro capítulo servirá de base para as reflexões do segundo capítulo. Pretende-se, então, enfrentar a legislação já existente no ordenamento jurídico brasileiro, a fim de aferir em que medida as novas tecnologias de informação e comunicação são reguladas, e se, ao fim e ao cabo, as nocividades da nova lógica se encontram reguladas, e, via de consequência, minimamente atenuadas. Para dar conta do serviço, o primeiro subcapítulo se debruça sobre a legislação infraconstitucional, notadamente o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD), ponderando os avanços e limitações da norma. A seu turno, o segundo subcapítulo enfrenta a jurisprudência do Supremo Tribunal Federal no julgamento das ADIs 6387, 6388, 6388, 6389, 6390 e 6393, e sobre a nova previsão expressa da proteção dos dados pessoais no rol de direitos fundamentais da Constituição introduzido por meio da Emenda Constitucional n. 115/2022, a qual inseriu o inciso LXXIX em seu art. 5º. Este subcapítulo busca, também, enfrentar a Emenda Constitucional como um todo, bem como investigar os reflexos do

relativamente novo *status* constitucional do direito à proteção dos dados pessoais. Ao final, pretende-se a reflexão acerca dos novos contornos e limites de atuação da norma constitucional.

Para tanto, foi utilizado o método de abordagem fenomenológico, adotado nas ciências jurídicas após a virada ontológico-linguística e adequada à investigação do fenômeno descrito por Shoshana Zuboff, pesquisadora e professora de Harvard. Por sua vez, o método de procedimento adotado foi o monográfico, lançando-se mão da técnica de pesquisa bibliográfica. Salienta-se não ter sido utilizado o método de procedimento histórico, pois sua utilização implicaria uma reflexão crítica acerca da (in)ocorrência dos eventos elencados ao longo do trabalho. Como não se pretende a verificação de fontes históricas, mas tão somente o enfrentamento dos reflexos sobre o usuário final, o trabalho se delimita ao método monográfico. A técnica de pesquisa utilizada foi a bibliográfica, por meio do exame de legislações, jurisprudências, livros e trabalhos científicos.

Ao longo da leitura, a monografia terá a característica de se debruçar demasiadamente sobre os feitos e estratégias do Google (empresa atualmente pertencente ao conglomerado Alphabet). Portanto, desde já é necessário advertir o leitor que o capitalismo de vigilância, sob o prisma adotado neste trabalho, se conformou a partir do Google e suas relações mantidas com outras empresas e o Estado americano, em uma época anterior ao Facebook, por volta do ano de 2005. Como se verá ao longo de desenvolvimento, a lógica vigente já se encontrava em estágio de avançada consolidação no momento da ascensão das demais empresas de tecnologia.

Dada a extensão da temática e a limitação ao número de páginas, este trabalho somente vai tecer algumas considerações sobre a ascensão do capitalismo de vigilância, algumas de suas notáveis características e sua repercussão em relação ao usuário final, sem a pretensão de esgotar a temática, especialmente em razão da volatilidade do assunto aqui tratado. Interdisciplinar por excelência, esta monografia pretende a interseção entre as ciências sociais e as ciências jurídicas.

Por fim, antes de adentrar o desenvolvimento deste trabalho, uma premissa deve ser fixada: por conta de o livro de Shoshana Zuboff compor o marco teórico desta monografia, as inúmeras referências ao trabalho serão meramente na pessoa da autora, ou ao “trabalho de Zuboff”, com apenas uma referência completa – a saber, a primeira. A obra da professora atuará como um fio condutor deste trabalho. Essa

medida se afigura adequada para manter a estética do texto, sem perder de vista a menção à produção da pesquisadora. Não obstante, as citações são em sua maioria indiretas, e a versão do livro utilizada foi a digital, que implica paginação irregular, de modo que uma referência completa única seguida de simples menções não é medida descabida ao trabalho. Ademais, a citação em idioma estrangeiro será livremente traduzida, a fim de garantir maior fluidez durante a leitura, com a inserção de nota de rodapé ao final com o trecho em seu idioma original.

2 O CAPITALISMO DE VIGILÂNCIA: UMA CONTEXTUALIZAÇÃO NECESSÁRIA

2.1 O SURGIMENTO DE UM SISTEMA INÉDITO

No ano de 2019, Shoshana Zuboff, pesquisadora e professora da Universidade Harvard, lança o livro “A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder”. A obra foi traduzida para o Português em 2020 e trazida ao Brasil pela Editora Intrínseca (ZUBOFF, 2020, p.i.). Resultado de anos de pesquisa, o trabalho da professora explora e sistematiza a ascensão do fenômeno do Capitalismo de Vigilância.

Logo no início, a autora assim define o fenômeno:

> **1.** Uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; **2.** Uma lógica econômica parasítica na qual a produção de bens e serviços é subordinada a uma nova arquitetura global de modificação de comportamento; **3.** Uma funesta mutação do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história da humanidade; **4.** A estrutura que serve de base para a economia de vigilância; **5.** Uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX; **6.** A origem de um novo poder instrumentário que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes para a democracia de mercado; **7.** Um movimento que visa impor uma nova ordem coletiva baseada em certeza total; **8.** Uma expropriação de direitos humanos críticos que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos. (ZUBOFF, 2020, p.i.) (grifos no original)

Essa definição, similar às encontradas nos dicionários, dá o tom de urgência em que a pesquisadora trata a temática ao longo de todo o livro. As nocividades da dinâmica do capitalismo de vigilância, melhor enfrentadas no subcapítulo seguinte, têm início em atividades muito simples, e que, na maciça maioria dos casos, ocorre

despercebidamente pelos usuários de produtos e serviços oferecidos pelas gigantes da tecnologia (as *Big Techs*). Porém, antes de iniciar o enfrentamento da teorização de Zuboff sobre o capitalismo de vigilância, propõe-se um exercício mental, a fim de introduzir e tornar mais facilitada a apreensão do conteúdo.

Pensemos em um carro. Esse carro pertence a João. Agora, pense no sistema de exaustão (escapamento) do carro. Por todos os lugares onde esse carro passa, o escapamento deixa resíduos de monóxido de carbono obtidos pela queima dos cilindros. Agora, imagine uma empresa especialista nesses sistemas de exaustão veicular. Digamos que essa empresa possua um sistema avançadíssimo, capaz de captar esses resíduos do sistema de escape, e, a partir deles, constatar por onde João passou, a que horário passou, de onde vinha, para onde estava indo, se estava com pressa, estressado e afobado, ou mesmo com calma e paciência, e se haviam pessoas junto com ele.

Quando João toma conhecimento dessa coleta e desse tratamento feito com esses dados de exaustão, fica um pouco preocupado, pois nem sequer imaginava que essas conclusões seriam possíveis, tampouco havia sido informado pela empresa que a coleta ocorreria e teria essa finalidade. João, então, entra em contato com a instituição, para saber por que esses dados estão sendo utilizados dessa forma. Em devolutiva, a empresa informa que João já consentira ao aceitar os termos de uso. Ainda, a instituição realiza a coleta desses dados – que seriam desperdiçados – e os utiliza para otimizar o trânsito e encontrar rotas alternativas em um GPS, ou mesmo para verificar a qualidade do ar e localizar alguma possível anomalia na exaustão do veículo. **Toda a atuação é voltada para garantir a melhor experiência do motorista João**.

Ocorre que, em determinado momento, quando João entra em seu veículo às 19h, seu telefone recebe uma mensagem SMS falando das inúmeras ofertas de uma loja pela qual João sempre passa em seu trajeto usual de retorno para casa após o trabalho. Ou, então, quando João se prepara para almoçar fora no sábado, enquanto navega em suas redes sociais, recebe inúmeras peças de publicidade de um restaurante novo que contém um cardápio muito semelhante ao do restaurante que João já frequentava.

Dias depois, João percebe que a empresa havia instalado sensores pela cidade, de modo que a captação de dados não ocorria mais apenas em relação à exaustão de seu veículo, mas também em relação às captações dos locais por onde

passava. A inteligência de máquina adotada por essa empresa permitia o entrelaçamento das informações obtidas pela exaustão de João, bem como a partir dos resultados dos sensores instalados nas localidades por onde João passou.

Após mais alguns dias, João nota que seu aplicativo de GPS começou a oferecer rotas alternativas, distintas da mesma que sempre utilizou para ir ao trabalho. Sob a alegação de haver melhores condições de trânsito, um novo trajeto lhe era oferecido, mas, ao conversar com seus colegas de trabalho, obtém a informação de que não havia engarrafamento em seu trajeto usual, mas havia uma loja em seu trajeto novo que pagava por anúncios.

João começa a se dar conta, então, que seus dados, coletados pela empresa de tratamento dos resíduos de exaustão, foram compartilhados com outras empresas, e vêm sendo utilizados para o fim comercial de estimular o consumo dos bens e serviços anunciados. E é assim, grosso modo, que funciona uma das facetas do capitalismo de vigilância.

Menezes Neto, Morais e Bezerra (2017), utilizando-se da construção do modelo panóptico de Bentham e Foucault, apontam que a vigilância não é fenômeno novo no curso da humanidade. Os autores sinalizam a ocorrência do *dataveillance*, um acrônimo de *data* (dados, em tradução livre do inglês) e *surveillance* (vigilância, em tradução livre do inglês), originado na década de 1980, definido como o “uso sistemático de sistemas de dados pessoais na investigação e monitoramento de ações e comunicações de um ou mais indivíduos” (MENEZES NETO, MORAIS, BEZERRA, 2017, p. 187-8). Com o passar do tempo, essa vigilância orientada por dados tomou novos contornos, resultando no que Shoshana chamou “capitalismo de vigilância”.

Em seu trabalho, Morais (2021), partindo da concepção de Estado Liberal Democrático de Direito, alertou para a necessidade de compreensão do fenômeno de maneira atrelada ao liberalismo, pois não se trata de casos dissociados. Deve-se compreender toda a conjuntura. O pesquisador rememora a constante tensão entre a política de inclusão – consubstanciada pelas políticas sociais – e a economia de exclusão vigente – capitalismo. Essas tensões, aliadas às inclinações de atuação estatal submetida ao cálculo econômico, refletem-se (negativamente) sobre as disposições da Constituição da República, especialmente na temática das garantias constitucionais. Um dos desdobramentos desse cenário é o aumento da judicialização das questões. O autor trouxe, ainda, o conceito de *New Surveillance*, vigilância

característica das sociedades hiperconectadas, muito além do sistema panóptico desenvolvido por Bentham e Foucault.

Adotando a nomenclatura “revolução da internet” de Stefano Rodotà, o autor aponta que não mais persistem

> as tradicionais fronteiras do Estado Nacional – geográficas (território) e institucionais (direitos e garantias) -, uma vez que a localização das informações armazenadas não necessariamente corresponde ao local de violação de um direito fundamental ou ao lugar de sede da empresa que guarda esses dados. Na realidade, na maioria das vezes os dados são armazenados simultaneamente em diversos pontos do globo com o intuito de fornecer redundância e acesso mais rápido aos usuários, independente de onde eles estejam localizados geograficamente. Não há mais coincidência entre o lugar da decisão política – Estado Nacional - e instância decisória – poder – e, com isso compromisso com os limites institucionais peculiares à fórmula Estado (Liberal) de Direito no que diz respeito a direitos e garantias clássicas – liberdade, privacidade, igualdade formal, contraditório, ampla defesa etc. (MORAIS, 2021, p. 24-5)

Mais adiante, o pesquisador discorre que, em decorrência desse fenômeno, o Estado, o Direito e o Estado Democrático de Direito vão sendo ressignificados, obedecendo a uma pauta que busca a maximização da eficiência, ocasionando o esvaziamento do sistema, e reduzindo-o à esfera econômica e monetária. E completa:

> Aqui, substituem-se as regras (do Direito) pelas normas (da Técnica) e o Estado de Direito se confronta com a perda de sua legitimidade clássica, talvez com o seu desaparecimento como tal, substituído por um “estado de direitos” – em minúsculas -cuja legitimação não está nem nas suas formas de produção, muito menos em seus conteúdos, sobretudo, de garantias, mas na eficiência dos resultados e na origem de seus regramentos e dispositivos, estes alicerçados em modelos referenciais técnicos. (MORAIS, 2021, p. 30-1)

Morais (2021) deixa antever, ainda, tópicos desenvolvidos por Shoshana Zuboff, e que serão enfrentados adiante: 1. A possibilidade de incitamento de conduta; 2. A prescrição de desejos; e 3. A coerção. Ao final, o autor arremata seu trabalho com o fenômeno da uberização do trabalho, e as perspectivas prejudiciais dele decorrentes, especialmente sobre os direitos sociais. No entanto, não haverá o aprofundamento da temática neste trabalho, pois estamos delimitados ao tratamento dispensado aos dados dos usuários.

Fornasier e Knebel (2021) descrevem o capitalismo de vigilância como produto do fenômeno do *Big Data*:

> O capitalismo do Big Data tem nos processos de coleta, armazenamento, controle e análise dos dados, a formação de um contexto de economia política que busca o controle econômico e político dos indivíduos, ao mesmo tempo em que os trata como consumidores ou potenciais terroristas/criminosos. Segundo Fuchs (2019, p. 58-59) o poder algorítmico do capitalismo de vigilância pode resultar em um mundo que seja um grande shopping center, com humanos colonizados completamente pela lógica comercial, no âmbito do seu comportamento. Portanto, há a ascensão de uma nova mercadoria, que não é fruto necessariamente do trabalho industrial: a mercadoria dos dados, que tem como base as plataformas de redes sociais, nas quais os usuários entregam seus dados em troca de serviços anunciado como gratuitos, mas que são transformados em mercadoria pelas empresas responsáveis pela sua oferta no mercado. (FORNASIER; KNEBEL, 2021, p. 1010)

O ano de 2002 é um marco temporal importante para o capitalismo de vigilância. Em seu trabalho, Zuboff disserta que foi a partir desse ano em que o Google – antes de fazer parte do conglomerado Alphabet – mudou sua tática de atuação no mercado, dando seus primeiros passos no capitalismo de vigilância. Anteriormente, a empresa de buscas possuía uma orientação econômica voltada à cobrança de valores por pesquisas no buscador. Contudo, em meio a uma crise econômica, com a concorrência indo em sentido diverso, a instituição deveria se reinventar se quisesse se manter no mercado. Assim, ao contragosto dos criadores da plataforma, a empresa passa a adotar a utilização de publicidade.

Com o passar do tempo, as táticas de publicidade do Google foram se aperfeiçoando até chegar a um ponto em que a publicidade estaria otimizada ao usuário mesmo se ocorresse uma navegação anônima, ou, ainda, baseada na inserção de informações falsas pelo utilizador. A pesquisadora argumenta que, a partir desse momento, massificam-se as violações dos direitos de autodeterminação do usuário.

Assim, é possível concluir que o capitalismo de vigilância começa a tomar forma em um contexto de instabilidade financeira, quando as autoridades dentro do Google abandonam os princípios morais iniciais e se avançam sobre o tratamento dos dados oriundos do que a autora chamou de superávit comportamental. Essa dinâmica, intrínseca ao capitalismo de vigilância, foi se construindo ao longo dos anos, conforme veremos a seguir. No entanto, para melhor compreender o fenômeno, é necessário dar um passo para trás.

Lembremo-nos sempre de que toda e qualquer utilização das tecnologias de informação e comunicação gera dados. Se nos idos de 1999 o Google mostrava-se um diferencial por aprender e otimizar os serviços a partir do *feedback* dos usuários,

a partir de 2002, a empresa vai aderir à captação e tratamento dos dados de exaustão.

Zuboff sinaliza existir entre os dois recortes acima uma distinção crucial. No primeiro, denominado pela autora "ciclo de reinvestimento do valor comportamental", a otimização era voltada única e exclusivamente à melhora da experiência do usuário. Um comportamento praticado no buscador – que gera dados comportamentais e exaustão de dados – tinha os dados comportamentais analisados, e a experiência do usuário final, aprimorada[2]. Esse momento foi assim descrito pela autora:

> Nos estágios bem iniciais do desenvolvimento do Google, os ciclos de feedback envolvidos no aperfeiçoamento das funções de busca produziam um equilíbrio de poder: a busca precisava das pessoas para aprender delas e as pessoas precisavam da busca para aprender dela. Essa simbiose possibilitava aos algoritmos da companhia aprender a produzir resultados de busca cada vez mais relevantes e abrangentes. Mais pesquisas significavam mais aprendizagem; mais aprendizagem produzia mais relevância. Mais relevância significava mais buscas e mais usuários. Na época em que a jovem companhia organizou sua primeira coletiva de imprensa, em 1999, para anunciar um investimento de capital de 25 milhões de dólares das duas mais reverenciadas firmas de capital de risco do Vale do Silício, a Sequoia Capital e a Kleiner Perkins, a busca Google já estava atendendo a sete milhões de pedidos por dia. (ZUBOFF, 2020, p.i.)

Como se vê, a tática inicial rendeu à instituição a confiança buscada por investidores, dado o aporte financeiro baseado no alto volume de buscas. Para fins de comparação, no ano de 1998, cerca de cem milhões de famílias estadunidenses estavam na internet (WEIL, 1999). Considerando-se a quantidade de buscas apontada no excerto acima, vislumbra-se o patamar expressivo da atuação do Google no mercado. Zuboff deixa antever que "ao longo dos anos seguintes, seria a captura, o armazenamento, a análise e a aprendizagem a partir dos subprodutos dessas buscas que transformariam o Google no padrão-ouro das buscas na internet" (ZUBOFF, 2020, p.i.). Nessa passagem, a autora indica o rumo que viria a ser tomado pela empresa a partir de 2002.

A pesquisadora explica que, a despeito da confiança depositada na instituição, a postura de reinvestimento do valor comportamental não propiciava auferir lucros aos investidores. O buscador concorrente Overture gerava receita a partir da compra de ranqueamento de resultados[3], implicando maior retorno aos capitalistas de risco da

[2] Fica o convite para que o leitor examine a Figura 1, que consta do Capítulo 3, item 2, de "A Era do Capitalismo de Vigilância".

[3] Em outras palavras, o mecanismo gerava receita ao vender a anunciantes os primeiros resultados que aparecessem em uma pesquisa realizada pelo usuário. Vale ressaltar que esta postura é adotada atualmente pelo Google.

época. No entanto, no ano 2000, o setor de tecnologia foi assolado por intensa crise financeira. A especulação gerada a partir da perspectiva de dinheiro rápido das "ponto-com"[4] fez que estourasse a "bolha da internet". O cenário era de pressão por lucro, implicando senso de emergência aos executivos do Google. É importante ressaltar, Shoshana alerta que o buscador do Google não deixara de ser utilizado. Em verdade, sua utilização seguia aumentando em larga escala, e existia um sem-número de candidatos interessados em algum cargo da instituição. Era o modelo de negócio em si que não gerava o lucro esperado. E foi em meio a essa crise que teve início a guinada da empresa rumo ao capitalismo de vigilância. Mais adiante, o trabalho dedicará um parágrafo para outro fator decisivo: a parceria com o aparelho estatal estadunidense. Porém, neste momento, devemos nos concentrar nas conformações do Google da época.

Os fundadores do Google, Sergey Brin e Lawrence "Larry" Page, como se deixou antever, não eram favoráveis à utilização de publicidade em momentos anteriores. Zuboff traz excerto de um trabalho realizado pelos empresários, no qual é possível depreender certo receio em relação a essa dinâmica:

> Imaginamos que os **mecanismos de busca financiados por publicidade sejam inerentemente parciais aos anunciantes e distantes das necessidades dos consumidores**. Esse tipo de parcialidade é muito difícil de detectar, mas ainda assim poderia ter um efeito significativo no mercado [...] **acreditamos que a questão da publicidade cause incentivos contraditórios suficientes para que seja crucial ter uma máquina de busca competitiva que seja transparente e esteja dentro do reino acadêmico**. (ZUBOFF, 2020, p.i.) (grifo e omissão nossos)

No entanto, como tempos desesperados requerem medidas desesperadas, o Google sutilmente alterou sua forma de atuação, de modo a gerar a receita esperada a seus investidores, e, via de consequência, manter-se no jogo do mercado por mais algum tempo – frise-se, o Google não apenas se mantém no mercado, como vem sempre listado entre as cinco maiores empresas de tecnologia do mundo, as *big five*. Chega-se, então, <u>ao segundo recorte</u> indicado linhas acima. A nova atuação do Google foi marcada por uma dinâmica quase oposta ao reinvestimento do valor comportamental:

[4] "ponto-com" (traduzido do original "dot-com", em inglês) é outro nome para empresas de tecnologia. Apesar de não ser sinônimo direto de *big tech*, para os fins deste trabalho não será necessária diferenciação minuciosa entre os termos.

> Para atender a esse novo objetivo [de geração de lucro aos investidores], o ciclo de reinvestimento do valor comportamental foi rápida e secretamente subordinado a uma empreitada maior e mais complexa. As matérias-primas que haviam sido usadas com o único intuito de melhorar a qualidade da busca agora seriam usadas também a serviço de dirigir a publicidade a usuários individuais. Alguns dados continuariam a ser aplicados no aprimoramento do serviço, mas os crescentes depósitos de sinais colaterais seriam reaproveitados para melhorar a lucratividade de anúncios tanto para o Google quanto para seus anunciantes. Esses dados comportamentais disponíveis para usos além de melhorias nos serviços constituíam um superávit, e foi declarado estado de exceção do Google foi o pano de fundo para 2002, o ano divisor de águas durante o qual o capitalismo de vigilância se estabeleceu de vez. (ZUBOFF, 2020, p.i.)

Ao longo da obra, a professora demonstra que a experiência do usuário ficou relegada ao segundo plano. Os reflexos da nova política do Google (e demais empresas de tecnologia que foram surgindo e se consolidando com o passar dos anos) indicam que o capitalismo de vigilância guarda pouca ou nenhuma relação com o inicial reinvestimento do valor comportamental. Muito embora não se possa falar em uma ruptura propriamente dita, o capitalismo de vigilância, conforme teorizado por Zuboff, inaugura uma nova dinâmica. Inédita, inclusive.

Shoshana defende que o atual estágio do capitalismo é figura inédita na história. Não houve fenômeno anterior que minimamente se assimilasse às dinâmicas propagadas pelo capitalismo de vigilância. Uma possível comparação seria em relação ao totalitarismo, porém, a autora de pronto sinaliza que a comparação é inadequada. Se de um lado, no totalitarismo, a teoria legitima a prática, no capitalismo de vigilância, a prática esconde a teoria[5]. O totalitarismo busca conformar a coletividade. O capitalismo de vigilância acontece por meio da exacerbação do indivíduo e da individualidade em detrimento do coletivo. De um lado, o totalitarismo busca o estabelecimento de uma identidade comum e prega uma religião política, ao passo que o instrumentarianismo[6], decorrente do capitalismo de vigilância, estimula comparação social por confluência e predibilidade, e prega a indiferença radical. Neste aspecto, faz-se necessária uma breve consideração. Indiferença radical pode ser entendida com a ausência de compromisso com alguma pauta, ou mesmo algum preceito ético. Conforme Meireles (2021),

[5] Ao longo do livro, Zuboff evidencia que a atuação das *big techs* sempre foi marcada pela pouca (ou ausência de) transparência. Via de regra, só se teve conhecimento das reais práticas das gigantes da tecnologia por meio de vazamentos e escândalos relacionados às companhias. Não é demais relembrar que os vazamentos trazidos por Edward Snowden, bem como o escândalo envolvendo o Facebook e a empresa Cambridge Analytica foram grande contribuição para o estudo desta matéria.

[6] Instrumentarianismo é definido por Zuboff como um movimento de instrumentalização do comportamento, para conseguir realizar sobre ele modificação, predição, monetização e controle.

> a indiferença radical em relação à visão coletivista da sociedade é observada quando o conteúdo da informação é julgado pelas empresas a partir de sua relevância em termos de números de cliques e curtidas, volume, profundidade e capacidade de gerar lucro. Não importa se o conteúdo é mentiroso, fraudulento ou contém discurso de ódio, desde que as pessoas cliquem nele. Os valores democráticos são ignorados para sustentar corporações de tecnologia e o sistema financeiro, que migra seus investimentos para esse setor (Dantas, 2019). O conteúdo não é avaliado conforme normas democráticas, como a livre imprensa, ou a liberdade de expressão, mas, sim, a partir dos termos de uso, determinados pelas empresas privadas. A suspensão de contas, ou retirada de conteúdos, dessas plataformas ocorre no tempo em que as próprias companhias determinam como adequado. (MEIRELES, 2021, p. 34)

Essas são algumas das características utilizadas por Zuboff para intentar uma comparação. No entanto, a autora alerta que empenhar muitos esforços em uma comparação poderia prejudicar a compreensão, o ajuste, e, eventualmente, a neutralização do que for nocivo. Ao fim e ao cabo, não devemos olhar para o fenômeno do capitalismo de vigilância buscando encontrar alguma característica ou semelhança com outro sistema já conhecido. Devemos, em verdade, enfrentá-lo com o ineditismo que lhe cabe, especialmente em relação às posturas das gigantes da tecnologia.

As práticas adotadas pelas *big techs* não são estanques. Os procedimentos vão se alterando com o passar do tempo, em constante avanço. Isto é, as práticas vivenciadas nos últimos cinco anos são quase distintas das do alvorecer deste século. Zuboff indica que, inicialmente, a sistemática de otimização de publicidade adotada pelo Google era fomentada, em sua maioria, pelas interações realizadas pelo usuário, o que se chamou *click-through* (taxa de cliques). Assim, quanto mais cliques recebia uma peça de publicidade, mais bem-sucedida e valiosa ela seria, e, por conseguinte, mais conteúdo parecido seria exibido ao usuário. Tempos depois, houve o surgimento da plataforma Google AdWords, cujo algoritmo levava em conta variáveis como a própria probabilidade de o usuário clicar em um anúncio. Nos últimos anos, viu-se ocorrer, também, a cessão onerosa de dados dos usuários a desenvolvedores/ instituições de terceiros, alheias à relação mantida entre utilizador e rede. Esses são alguns exemplos das práticas realizadas. Reservam-se, contudo, essas práticas, especialmente as de tratamentos de dados mais recentes para o próximo subcapítulo, oportunidade em que serão contrastadas com os reflexos por elas gerados.

Desde já, olhos atentos perceberão existir certa similaridade nas atuações das empresas de tecnologias. É possível afirmar que não se verão posturas

diametralmente opostas na condução dos trabalhos de uma gigante da tecnologia. Zuboff defende que isso se deve ao novo capitalismo. A autora alerta que, antes do Google e quaisquer das *Big Techs*, o que persiste é a lógica do capitalismo de vigilância no pano de fundo. Isto é, não devemos pôr em um mesmo patamar as empresas de tecnologia e a lógica do capitalismo. A autora propõe uma dissociação entre os dois. Com isso, independentemente das práticas adotadas pelas gigantes da tecnologia, é possível antever que as inovações obedecerão, em maior ou menor grau, ao imperativo de predição[7], decorrente do capitalismo de vigilância. A fim de ilustrar melhor sua colocação, a pesquisadora de Harvard se utilizou da analogia com marionetes. As empresas de tecnologia, no auge de toda a sua atuação e todos os reflexos que exercem sobre os usuários, nada mais são do que reles marionetes. E o titeriteiro[8] é o próprio capitalismo de vigilância. Dessa forma, a atuação estará sempre atrelada, e, por óbvio, orientada pela lógica do titeriteiro. Com isso, pode-se concluir que novas empresas e novos produtos/serviços não serão, ao fim e ao cabo, muito diferentes dos existentes hoje, especialmente em termos de captação, análise e tratamento de dados. As práticas podem se alterar, mas a captação, análise e tratamento de dados não deixarão de existir. Não à toa, mais adiante, a professora manifestará que melhores condições de utilização da tecnologia serão possíveis somente por meio do combate à lógica vigente. Não nos adiantemos muito. A temática será oportunamente enfrentada no próximo subcapítulo.

Como apontado linhas acima, a utilização de um serviço implica a geração de dados. A partir dos novos rumos tomados pelo Google em relação à publicidade, a exaustão de dados, antes não aproveitada, passou a ser de grande valia à instituição. Ao longo dos anos, os mecanismos utilizados – tanto pelo Google quanto as demais empresas de tecnologia despontantes – foram objeto de sucessivos aprimoramentos. Os dados de exaustão, outrora ignorados, tornaram-se objeto de tratamento[9], resultando no que Zuboff chamou de superávit comportamental. Esse produto permitia a seu detentor passar à frente da concorrência em relação aos produtos de

[7] Em sua obra, Shoshana Zuboff argumenta existir busca incessante pela eliminação da dúvida e estabelecimento da certeza. Isso ocorrerá a partir do aperfeiçoamento da capacidade de predição dos algoritmos, daí falar-se em "imperativo de predição". A ideia também é difundida entre as gigantes da tecnologia como forma de driblar as instabilidades inerentes ao capitalismo. No entanto, um dos desdobramentos dessa postura é a violação da privacidade dos usuários, e, por conseguinte, sua liberdade e direito à autodeterminação.

[8] Titeriteiro é a pessoa quem controla as marionetes.

[9] Zuboff atribui o nome de renderização ao tratamento de dados. A prática consiste, grosso modo, no aproveitamento dos dados gerados pelo utilizador para os fins a que se destinam.

publicidade ofertados. Com efeito, o superávit comportamental permite maior acurácia na destinação de uma peça de publicidade ao utilizador.

Até aqui, muito se falou sobre a consolidação das *big techs*. Porém, uma menção se faz fundamental para a compreensão da ascensão do capitalismo de vigilância: as "parcerias" do Google com o Estado americano. Após os atentados ocorridos no episódio do 11 de setembro, instalou-se um ambiente de "guerra ao terror", em que a privacidade dos dados dos usuários poderia ser suprimida a fim de garantir segurança aos cidadãos estadunidenses. O sistema Google Maps (e o ocorrido com o *Street View*, enfrentado no subcapítulo seguinte), por exemplo, surgiu da aquisição da empresa de Keyhole em 2003. A instituição era, anteriormente, subsidiada pela CIA para realizar o mapeamento geográfico do planeta (MEIRELES, 2021). Meireles (2021) sinaliza, ainda, que esse cenário, somado à transição do capitalismo de mercado ao neoliberalismo – este marcado pela ausência de regulação no setor da tecnologia –, não permitia grandes avanços em termos de direitos de privacidade do utilizador. A autora aponta que, à época, qualquer contestação em favor da positivação de direitos de privacidade era vista como uma interferência no mercado e na inovação tecnológica.

Para Morais (2021), esse momento, marcado pela "guerra ao terror", foi crucial para a expansão e consolidação do capitalismo de vigilância. Com efeito, o momento foi oportunamente utilizado para o lançamento da captação massiva de dados:

> O motto para a coleta, armazenamento, tratamento e análise massiva de dados, como se sabe, foi a "guerra contra o terror", muito embora não se tenha evidências de nenhum caso concreto em que esse uso da tecnologia tenha efetivamente abortado uma ameaça terrorista iminente, embora tenha servido para outros fins, como a guetização de grupos, a catalogação e persecução de indivíduos, o controle de fluxos migratórios etc. Agora, estas mesmas práticas explicitam a fragilidade, bem como a submissão da democracia a tais instâncias "secretas" de poder capazes de influenciar e até mesmo alterar o resultado das práticas democráticas clássicas – as eleições ou instrumentos de participação popular (referendum ou plebiscito) – construindo e/ou desvirtuando maiorias eleitorais (caso Trump) ou opções políticas pontuais (caso Brexit). "Corrompendo", assim, a própria democracia e, ao final, o Estado (Liberal) de Direito.
> Embora tenha demonstrado ser pouco eficiente para prever e neutralizar ataques terroristas, esse "mau" exemplo explicita uma característica desta nova "era da quantificação", impregnando todos os setores – das práticas mercadológicas às escolhas eleitorais e, com isso, põe em xeque o próprio Estado (Liberal) de Direito. (MORAIS, 2021, p. 25-6)

Com o passar do tempo, a despeito de eventos emblemáticos, como as declarações de Edward Snowden, a busca pelo superávit comportamental manteve

seu curso. E, consolidada como está, a lógica de eficiência na predição de comportamentos e interesses, bem como a busca pela otimização desses mecanismos, vêm trazendo reflexos negativos. A lógica se mantém. De toda sorte, novas posturas surgem, e, com elas, violações de direito as mais variadas, como veremos agora.

2.2 AS NOCIVIDADES DO SISTEMA E O ESTADO DA ARTE

Por trás das gigantes da tecnologia está o capitalismo de vigilância. Por trás das marionetes, o titeriteiro. Até aqui, foi possível inferir algumas das nuances do capitalismo de vigilância. Neste subcapítulo, serão enfrentados os desdobramentos práticos dessa lógica vigente, consubstanciados pelas gigantes da tecnologia. No momento em que este trabalho está sendo construído, o mundo chama as cinco maiores empresas de tecnologia de *big five* (as cinco grandes, em tradução livre). São elas: Meta (atual conglomerado detentor do Facebook), Amazon, Microsoft, Apple e Alphabet (conglomerado detentor do Google). Além de possuir lobby nos Estados Unidos a fim de suprimir concorrência, essas instituições adotaram posturas que, como veremos nas próximas páginas, não são entendidas adequadas e violam diversos direitos dos utilizadores, e, em alguns casos, de não-utilizadores. Aliás, o lobby por elas mantido também busca a manutenção de suas práticas, barrando o avanço de pautas de privacidade digital e consequente contenção do capitalismo de vigilância (MEIRELES, 2021).

O superávit comportamental é um dos principais desdobramentos do imperativo de predição. No entanto, com o passar do tempo, a exaustão de dados não era mais suficiente para satisfazê-lo. Os dados do mundo *on-line* já não eram preditivos o suficiente. Zuboff pontua que a etapa seguinte de obtenção do superávit comportamental foi a partir do mundo físico. A título de exemplificação, menciona-se o caso envolvendo o sistema *Street View* do Google. O projeto iniciado em 2007, na forma como anunciado pela empresa, era composto de veículos que percorreriam as ruas com câmeras fotográficas responsáveis pela captura de imagens. Posteriormente, tais imagens seriam unidas e utilizadas para propiciar uma visão da rua ao utilizador da aplicação. Ocorre que, no ano de 2010, autoridades alemãs reportaram que o veículo não capturava apenas imagens das ruas, mas também – e de maneira sigilosa – os dados pessoais das redes Wi-Fi privadas. Zuboff traz que

> Peritos técnicos no Canadá, na França e na Holanda descobriram que os dados de *payload* incluíam nomes, números de telefone, informação sobre crédito, senhas, mensagens, *e-mails* e transcrições de bate-papos, bem como registros de namoros *on-line*, pornografia, comportamentos de navegação na *web*, informação médica, dados de localização, fotos e arquivos de vídeo e áudio. Concluíram que tais pacotes de dados podiam ser costurados e formar um perfil detalhado de uma pessoa passível de ser identificada. (ZUBOFF, 2020, p.i.) (grifo nosso)

A comoção sobre escândalo de "Spy-Fi" [10] do Google rendeu investigações e sanções à empresa. Ao fim e ao cabo, Google apontou ter tudo ocorrido em razão de um erro de programação. Zuboff explica que essa é uma das táticas das gigantes da tecnologia durante o ciclo de despossessão (adiante enfrentado), na qual se atribui a alguém a responsabilidade de um "erro"[11], e, livrando-se de tal pessoa, livra-se do "erro" e a instituição mantém ares de integridade e ética em relação ao público.

Todavia, a busca pelo superávit comportamental também não se limita ao mundo físico. A etapa seguinte, consoante a teoria de Shoshana Zuboff, é a captação a partir da vida cotidiana. Sob a bandeira da "personalização", assim exposta pela pesquisadora, novas violações acontecem em relação ao utilizador. Com o passar do tempo, cada aspecto da experiência humana passa a contar em favor do imperativo de predição, com o mote de garantir cada vez mais certeza. Se antes os dados de navegação eram fundamentais, chega-se a um ponto em que não são mais suficientes, fazendo-se necessária aos interesses das *big techs* a cada vez maior consciência sobre usuário, mesmo que isso signifique violar sua privacidade.

Não se limitando à vida cotidiana, a etapa seguinte da busca pelo superávit comportamental ocorre sobre o corpo e identidade do utilizador. A autora aponta que o corpo do utilizador passa a se tornar uma fonte de extração de dados:

> O seu corpo é reimaginado como um objeto se comportando para ser rastreado e calculado para indexação e busca. A maioria dos aplicativos de smartphone exige acesso à localização do usuário mesmo quando não é necessário para o serviço que fornecem, apenas porque a resposta a essa pergunta é muito lucrativa. (ZUBOFF, 2020, p.i.)

Desse setor da extração de dados – e consequente renderização – decorrem

[10] O termo deriva do inglês "espionar" (*spy*) e Fi (de Wi-Fi), em construção decorrente da espionagem realizada por meio da captação de dados das redes Wi-Fi.

[11] Após novas investigações, constatou-se que a captura de dados das redes dos moradores foi de conhecimento dos engenheiros de software, que, mesmo cientes, mantiveram a orientação do algoritmo.

as peças de publicidade enviadas ao utilizador com base em sua localização, a partir de uma técnica que explora a compulsão do consumidor. A autora aponta que diversos aplicativos utilizam os serviços de localização do usuário mesmo que isso não seja útil ao funcionamento da aplicação. Ainda, trouxe dados do aumento de utilização de aplicativos que exigiam a permissão para utilizar serviços de localização. De 2013 para 2015, o percentual de utilizadores saltou de 74% para 90%. Esse aumento pode ser explicado pela dependência da tecnologia, e vem se justificando por meio de termos de uso capazes de permitir a extração de dados dos usuários. Termos esses compostos por belas palavras, mas que, em termos práticos, são “termos de rendição” na concepção de Zuboff.

Por fim, os levantamentos da professora de Harvard apontam a última etapa da captura de superávit comportamental por meio do comportamento modificado. Quando não há mais dados para extrair do usuário, isto é, quando os dados já foram exaustivamente tratados/renderizados, a etapa seguinte é a modificação do comportamento. Sob uma perspectiva behaviorista, Zuboff discorre sobre como aplicações – especialmente as utilizadas em *smartphones* – trabalham na função de alterar o comportamento dos utilizadores. O exemplo mais marcante trazido pela pesquisadora é o fenômeno do Pokémon Go, criado pela Niantic, empresa do Google. Em síntese, o aplicativo reúne os entusiastas do mundo de seres fantásticos, e, por meio da utilização de realidade aumentada, possibilita a visualização dos monstrinhos através das lentes do celular, como se estivessem no mundo real, e permitem ao jogador capturá-los. Ainda, para aumentar o engajamento dos jogadores, foram criados ginásios (iguais aos da série de animação japonesa), onde o jogador pode competir e vencer o líder, como fazia o personagem principal, Ash Ketchum. Um dos diferenciais[12] do jogo é que, para encontrar os Pokémons, o jogador deve se locomover pelo espaço. Isto é, trata-se de um jogo móvel para ser jogado no mundo real. Como assertivamente apontado por Shoshana, não tardou até que o capitalismo de vigilância se fizesse presente na aplicação. Com a recordista difusão do jogo, logo se viu surgirem ginásios em localidades específicas, dentro de restaurantes, por exemplo, que haviam adquirido a localização do ginásio, como forma de atrair possíveis clientes. Ou seja, estabelecimentos pagaram para que houvesse, por

[12] Fala-se em diferencial por conta da ampla aceitação e utilização do jogo eletrônico. No entanto, o Pokémon Go não é um jogo inovador por si só. Antes dele, já existia o jogo Ingress, produzido pela Niantic Games, pertencente ao conglomerado Alphabet, que possui a mesma dinâmica de utilização.

exemplo, um ginásio próximo – ou mesmo dentro – de seu estabelecimento, de modo a atrair os jogadores. Dessa forma, sutilmente o comportamento do utilizador/jogador era conformado ao interesse da empresa.

Arafan (2021) realizou, sob o pano de fundo do capitalismo de vigilância, um estudo exploratório das informações do aplicativo Pokémon Go e as nuances da aplicação ao longo do jogo e da interação do usuário. O objetivo era observar as variações de relevância no jogo em relação à localização; o efeito dos elementos textuais da aplicação nas inclinações dos usuários; e em que medida a Niantic tentava gerar alteração comportamental nos usuários e se a medida era lucrativa. O autor leva em conta três setores: a tela, representando todo o aspecto tecnológico, como o serviço de geolocalização e a realidade aumentada; o texto, representando as informações dentro do jogo, como Pokéstops, ginásios etc.; e o espectador, representando o jogador, em que se busca verificar qual extensão da modificação comportamental e lucratividade da medida. O principal resultado obtido pelo pesquisador foi que

> Embora Pokémon possa trazer mérito ao jogador nos três setores do dispositivo, o objetivo-fim do jogo sempre será um método opaco de modificação. Isso viola as recomendações de Hebing em relação tanto ao Big Data quanto às tecnologias manipulativas. Portanto, a partir da experiência de jogo sob o pano de fundo da literatura sobre capitalismo de vigilância, Pokémon Go confirma a definição crítica trazida por Zuboff a respeito do capitalismo de vigilância. (ARAFAN, 2021, p. 46)[13]

Meireles (2021) possui uma visão mais atenuada sobre as táticas de modificação comportamental. Em seu trabalho, a autora aponta que a formação das preferências e escolhas individuais é um processo complexo de subjetividade. Ainda, rememora o atual contexto de cultura do compartilhamento, em que a publicização da vida privada atua como um processo de autoafirmação, em um reforço da identidade de um indivíduo. O artigo também pontua que a tentativa de modulação do comportamento não é uma exclusividade das TICs, quanto menos tenha começado com elas. Por conta dos procederes obscuros adotados pelas empresas de tecnologia, não é possível aferir com precisão o potencial de modificação

[13] Trecho originalmente em inglês, livremente traduzido. Trecho original*: Although Pokémon Go can bring virtue to the players on each of the steps of the dispositif, the end-goal of the game will always be an opaque method of commodification. This violates Hebing's recommendations concerning both Big Data and manipulative technologies. Therefore, through my literature-backed gameplay, Pokémon Go confirms Zuboff's critical definition of surveillance capitalism.*

comportamental. Ao fim e ao cabo, mesmo que distanciando-nos da perspectiva *behaviorista* adotada por Zuboff, o trabalho de Meireles conclui que ainda existem, sim, reflexos sobre o comportamento dos usuários, podendo variar de caso a caso.

Diante do exposto até aqui, é possível concluir que as posturas adotadas pelas gigantes da tecnologia, orientadas pela lógica do capitalismo de vigilância, refletem nocivamente no usuário final. Em um primeiro momento, pela quebra da expectativa da privacidade do utilizador, tanto pela própria utilização desvirtuada dos dados gerados ao longo da navegação, quanto pela utilização posterior, não prevista nos termos de uso. Em um segundo momento, como desdobramento, pela utilização dos dados do usuário e do ambiente ao seu redor do utilizador para não apenas otimizar a publicidade, mas intentar modificar seu comportamento. Independentemente do grau de influência, a mera intenção de alterar comportamentos e inclinações permite-nos inferir existirem prejuízos à autodeterminação do usuário. Não se pode olvidar que não se conhece a totalidade dos processos que ocorrem no tratamento de dados dos utilizadores. Portanto, é seguro afirmar que a autodeterminação do indivíduo se vê ameaçada. Nesse sentido, Meireles (2021) defende a regulação dos algoritmos e das *big techs* com urgência, com vistas a defender a própria democracia liberal:

> É necessário regular o funcionamento dos próprios algoritmos. Esses códigos são o outro lado da moeda no debate sobre proteção de dados pessoais e privacidade. Compreender como funcionam é central para inferir seus impactos nas sociedades, ainda que a simples abertura dos códigos não signifique que seja possível controlar seus efeitos. A transparência é apenas um passo para compreender a complexidade de suas repercussões, além de ser complementar ao debate sobre proteção de dados pessoais e privacidade. Os algoritmos não são neutros, são instrumentos que operam de acordo com finalidades predeterminadas. Justamente por isso suas decisões não são tomadas com base em análises isentas, ou critérios de justiça, mas operadas de acordo com interesses, em sua maioria comerciais. Por isso a urgência de haver transparência sobre a forma como operam, em especial quando as pessoas estão sujeitas às decisões tomadas por eles.
>
> É precisamente nesse sentido que a ausência de regulação dos algoritmos ameaça as democracias liberais. Ao se colocarem como intermediários dos processos de decisão, eles reforçam assimetrias e preconceitos de raça, gênero e renda. O fenômeno pode ser observado na seleção prévia e categorização realizadas por setores, como planos de saúde, obtenção de crédito e o próprio sistema de segurança pública. Ao deslocar o poder decisório para os algoritmos, ocorre uma ruptura com a própria lógica do Estado democrático de direito, essencial para as democracias liberais. (MEIRELES, 2021, p. 42)

Em que pese tenha-se referido que as gigantes da tecnologia sejam marionetes obedecendo à lógica do titeriteiro, não se pode pô-las em uma posição de instituições

inocentes e manipuladas. Ao longo de seu livro Zuboff discorreu sobre uma metodologia adotada pelas *big techs*, a qual atribuiu o nome de ciclo de despossessão. Esse ciclo corresponde aos esforços das empresas de tecnologia na manutenção da renderização do superávit comportamental.

Como visto anteriormente, as práticas das gigantes da tecnologia ferem a privacidade e a própria autodeterminação dos usuários. No entanto, sob a lógica do capitalismo de vigilância, os direitos pouco importam. O que se busca é a certeza, seguindo o imperativo de predição. Mantêm-se, portanto, os procedimentos, independentemente da nocividade das práticas. Contudo, como ocorreu com o Google *Street View*, as práticas nocivas de extração de dados podem virar notícias, e, ao fim e ao cabo, prejudicarem a imagem das gigantes da empresa. E, em casos tais, vislumbra-se o ciclo de despossessão, composto por quatro etapas: incursão; habituação; adaptação; e redirecionamento. Em seu livro, Zuboff, utilizou como exemplo o escândalo do *Street View*.

A primeira etapa consiste na introdução/incursão do serviço captor aos utilizadores. Em caso de resistências e/ou oposições, procura-se naturalizar/habituar a aplicação, seja por meio de colocações tranquilizadoras, seja pelo fator tempo decorrente de longos processos judiciais, correspondendo à segunda etapa. E, enquanto o tempo passa, a instituição continua a executar os serviços danosos, e mesmo a aprimorá-los. Acaso permaneça a resistência ao serviço – ou mesmo com a superveniência de uma cominação a alterar o serviço –, a empresa de tecnologia realiza algumas alterações superficiais e imediatas e as divulga como se fossem a solução aos problemas da aplicação. Contudo, essa terceira etapa, de adaptação, não altera o cerne dos problemas encontrados no serviço, de modo que a extração de dados permanece incólume. Ao final, a etapa do redirecionamento tem a ver com os esforços das *big techs* em desenvolver novas retóricas que justifiquem a extração de dados. Isto é, novas retóricas para a não tão nova lógica de obtenção de superávit comportamental.

Conforme ao já exposto nas páginas anteriores, quando o utilizador/consumidor toma conhecimento das nocividades a que está sujeito, obtém da instituição a justificativa de que o tratamento dos dados se reverte em melhoria dos serviços. Para mais, assim dirão as gigantes da tecnologia: *em primeiríssimo lugar, o consumidor já estava de acordo com os termos de uso do produto/serviço utilizado, pois bem no início havia marcado a opção "estou ciente e quero continuar"*. Quando as *big techs*

argumentam a respeito de violações, buscam tornar a discussão meramente contratual, ofuscando o caráter fundamental do direito à proteção dos dados pessoais do utilizador.

Essa postura mitigadora de violações não é tida como uma surpresa. Pelo contrário, ela corresponde em muito às posturas das gigantes da tecnologia. Shoshana argumenta que as empresas são marcadas por procedimentos obscuros que vêm a conhecimento somente em casos de vazamento. Ao tomarmos como exemplo o caso do *Street View*, trabalhado acima, temos que o conhecimento sobre a extensão da captação dos dados de redes Wi-Fi somente ocorreu após investigações de diversos países. Nunca houve qualquer menção por parte da empresa. E, vendo recair sobre si uma reputação decadente, a instituição procurou tornar o ocorrido um erro, atribuindo a culpa a um dos engenheiros de software da empresa. Com a demissão desse bode expiatório, a empresa poderia buscar manter uma aura de ética e profissionalismo, e que a referida violação teria sido um ponto fora da curva. Vale relembrar que, tempos depois, veio a público a informação de que a captura dos dados das redes Wi-Fi não era um ponto fora da curva, mas um fato de amplo conhecimento dentro da instituição, que nada fez senão aproveitar aquilo como uma oportunidade.

Outra tática amplamente utilizada pelas gigantes da tecnologia é a utilização de novas palavras para abrandar seu reflexo potencial. Na época da popularização do superávit comportamental e início das críticas à postura do Google, seus representantes atribuíram o nome de dados de exaustão (*data exhaust* no original em inglês) e migalhas digitais (*digital breadcrumbs* no original em inglês). A perspectiva é a de diminuir o real potencial nocivo desses institutos. Chamar de dado de exaustão remete à ideia de algo que já existia por si só e seria perdido, mas que passou a possuir alguma serventia. Quanto às migalhas, remete-se à ideia de insignificância, e, portanto, inofensividade. Ao fim e ao cabo, intentava-se, também, afastar a ideia de que o tratamento desses dados poderia implicar violações diversas aos direitos dos utilizadores.

Zuboff também rememora ter havido casos em que, diante da cominação em esclarecer procedimentos adotados, as gigantes da tecnologia optam por permanecer silentes. Ainda, as empresas preferem ser sancionadas financeiramente (frise-se que se trata de alto valor pecuniário) a ter de compartilhar as técnicas por si adotadas. Para além da justificativa de evitar dar à concorrência o *know-how* dos algoritmos e/ou

procedimentações, a postura das gigantes da tecnologia permite uma suposição no sentido de que há muito mais ocorrendo dentro dos escritórios do que de fato se tem conhecimento. No entanto, não são necessárias grandes elucubrações sobre o que pode se passar nas sedes das gigantes do Vale do Silício. Os ocorridos dos últimos anos permitem boa compreensão do estado da arte.

Além dos eventos relacionados ao *Street View*, este trabalho não pode deixar de enfrentar – mesmo que brevemente – o ocorrido em relação a Cambridge Analytica e as interferências nas eleições dos Estados Unidos da América, enfrentado pelo trabalho de Martins e Tateoki (2019). Muito embora não se desconheça a interferência russa (ACEVES, 2019), a empresa de consultoria política foi decisiva no pleito que elegeu o republicano Donald Trump. A empresa lançou mão da coleta de dados realizada pelo Facebook, por meio das concessões realizadas pelos usuários ao aceitar os termos de uso de um aparentemente inofensivo teste de personalidade, chamado *thisisyourdigitallife*. A extração de dados dos usuários ocorreu em junho de 2014. Munida de grande quantidade de dados, a empresa traçou perfis dos usuários e direcionou, por meio de propaganda, conteúdo midiático otimizado a cada um deles, de modo a garantir maiores chances de obter o voto no então candidato do Partido Republicano. Estima-se que tenha havido a captura de dados de cerca de cinquenta milhões de usuários estadunidenses (THE GUARDIAN, 2018). É importante ressaltar que a extração dos dados ocorreu em 2014, porém as investigações do caso só tiveram início em dezembro de 2016, e o caso veio a público apenas em março de 2018. Nesse meio-tempo, houve solicitações da assessoria jurídica do Facebook ao cientista de dados Christopher Wylie que destruísse as cópias dos dados coletados. Cambridge Analytica despendeu mais de um milhão de dólares para coletar os dados dos usuários. Este caso representa um evento em que foi possível desvelar as práticas obscuras de uma empresa de tecnologia, e compreender seus procedimentos e os resultados do tratamento desenfreado de dados pessoais. O trabalho de Martins e Tateoki (2019) também aponta que não houve, no caso, a utilização da aplicação por cinquenta milhões de usuários. Contabilizou-se, em verdade, cerca de 270.000 usuários que realizaram o teste da aplicação. No entanto, o tratamento dos dados desses utilizadores permitiu obter informações precisas sobre os 50 milhões de usuários, em razão da política flexível do Facebook da época, que permitia compartilhar informações dos perfis dos utilizadores com instituições terceiras. Ainda, os autores sinalizam que algumas dezenas de curtidas na rede social Facebook já

são suficientes para que um algoritmo compreenda boa parte das preferências do utilizador. Como veremos mais adiante, essa precisão prejudica a possibilidade de anonimização do usuário.

Ainda sobre a conformação social promovida pelos algoritmos, o trabalho de Aceves (2019), acima referido, apesar de se dedicar a enfrentar a influência russa sobre o movimento *Black Lives Matter*, fornece profícuo panorama sobre a utilização das TICs por um Estado a fim de fragilizar outro. Após contextualizar os atritos já existentes entre os Estados Unidos da América e a Rússia, o autor descreve como os serviços de inteligência russa utilizaram redes sociais como o Facebook, Instagram e Twitter para o fim de fragilizar estruturas sociais estadunidenses. Nessas redes foram criadas contas cujo conteúdo publicado se identifica ao longo de todo o espectro político de esquerda-direita. Isto é, a contrassenso, houve a criação e a popularização de páginas que defendem as pautas das minorias, como o movimento negro e o movimento LGBTQIA+. Em relação ao *Black Lives Matter*, o autor apontou que foram criadas páginas favoráveis e contra o movimento, e, após adquirirem notoriedade e alguns milhares de seguidores e preciosa influência, cada uma delas convocou uma manifestação na mesma data e local, a fim de fazer estar no mesmo lugar dois pontos antagônicos. O autor conclui que a intenção era fragilizar bases sociais dos Estados Unidos da América, país em que o racismo é pauta de constante desarmonia. Não se pretende, neste trabalho, porém, enfrentar as razões e os posicionamentos do movimento, pois tal tarefa demandaria um trabalho inteiramente dedicado à temática. Não se desconhece, ainda, o tom de autopiedade em que o autor insere os EUA em relação à Rússia seu trabalho. Para os fins desta monografia, enfrentou-se apenas a utilização das TICs pela inteligência russa como forma de atacar um Estado, inflamando setores da sociedade e causar caos. Eventos como o presente são boa ilustração da faceta de indiferença radical. Aos capitalistas de vigilância não interessa se as tecnologias são utilizadas para fins de incentivo de ódio e cisão da sociedade. Ou, em um recorte mais distanciado, pouco importa ao capitalismo de vigilância se as TICs são utilizadas como arma de guerra, em esforços de fragilizar a estrutura social de um país. Consoante visto anteriormente, em havendo retornos em pecúnia, negócios são celebrados, sem grandes preocupações com os reflexos gerados ao longo do processo (MEIRELES, 2021).

Camurça e Matias (2021) revisitam três casos emblemáticos relacionados à discriminação por meio do tratamento de dados: Target, ViaQuatro e Decolar.com. O

caso da empresa Target consistiu no tratamento de dados dos consumidores, quando houve o envio de cupons de desconto a uma consumidora ainda adolescente, expondo sua gravidez a sua família, que ainda não tinha conhecimento. No caso da empresa ViaQuatro, a concessionária responsável pela linha amarela do metrô de São Paulo utilizou reconhecimento facial para identificar se os passageiros estavam consumindo as publicidades dispostas nos vagões. Porém, os referidos dados (biométricos) são considerados sensíveis pela LGPD, de modo que se faz necessário o consentimento explícito do titular. Foi ajuizada uma Ação Civil Pública pelo Instituto de Defesa do Consumidor (IDEC), para impedir a coleta massiva de dados. Por fim, o caso da empresa Decolar.com envolveu *geoblocking* e *geopricing*. A primeira conduta se refere a impossibilitar a compra de passagens aéreas ou demais produtos/serviços em razão da localização em que está o utilizador. A segunda conduta corresponde à prática de preços diferentes para um mesmo produto/serviço em relação a consumidores situados em localidades distintas. A empresa foi sancionada em R$ 7.500.000,00 pela prática discriminatória, que violou frontalmente o princípio da boa-fé, também previsto na LGPD.

Os autores, ao arrematar seu trabalho, tecem considerações sobre o novo molde de negócios digitais emergentes, bem como a forma como os direitos dos titulares são violados:

> Nos novos modelos de negócios digitais, a publicidade útil e direcionada se faz essencial para o aumento de consumo de produtos e de serviços. Tornou-se necessário captar as ânsias de uma geração e convertê-las em verdadeiros objetos de desejo. As informações pessoais, assim, tornaram-se altamente relevantes para personalização da experiência. Essa personalização, contudo, resta maculada quando realizada por práticas ocultas de rastreamento do usuário, como os supercookies e o fingerprinting. Elas violam frontalmente os sete fundamentos estabelecidos sobre a disciplina da proteção dos dados pessoais no Brasil, tais como o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, da honra e da imagem. (CAMURÇA; MATIAS, 2021, p. 21)

Os eventos trazidos neste trabalho evidenciaram inexistir um controle concreto/efetivo sobre o conteúdo difundido por meio das tecnologias de informação e comunicação, especialmente no que toca às plataformas de redes sociais. Aliás, conforme defendido por Zuboff, há pouco conhecimento sobre as práticas adotadas por empresas de tecnologias, e, do pouco que se sabe, grande parte se desdobra em elementos nocivos ao usuário. Atualmente, a proteção dos dados pessoais dos usuários adquiriu o status de direito fundamental. E, nesse novo contexto, se, em

princípio, as gigantes da tecnologia não se opunham ao *status* constitucional, após a edição de projeto de lei que busca regular empresas de tecnologia, as *big techs* se rebelaram. Durante a construção deste trabalho, houve o lançamento do projeto de lei n. 2630/2020[14]. Frias e Nóbrega (2021) enfrentaram o projeto. Sob o panorama de crescente difusão de notícias falsas (ou desinformação), especialmente após 2016, as autoras sinalizam ter havido movimento legislativo em diversos países no sentido de regular a difusão da (des)informação. Após argumentar sobre as concepções de "verdade", as autoras alertam para a necessidade de regulação da difusão dos conteúdos, assim sintetizando o projeto:

> O texto inicial do projeto da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, se propunha a reafirmar a verdade e a autoridade do jornalismo por meio do controle de um conteúdo definido como desinformativo. Ao longo de sua tramitação, após pressões de diversos grupos sociais, o projeto deixa essa narrativa e passa a olhar a desinformação do ponto de vista de seus elementos estruturais e comportamentais, buscando restabelecer a integridade do debate público com base no combate ao comportamento inautêntico e às redes de disseminação de desinformação. De pano de fundo, a leitura a respeito do papel das plataformas no fenômeno da desinformação permanece em ambos os textos, com regras que visam regular sua arquitetura e atuação. (FRIAS; NÓBREGA, 2021, p. 390)

O projeto ganhou notoriedade no ano de 2023, quando gerou manifestos lançados pela gigantes da tecnologia. O Google manteve na página inicial do buscador o *link* para seu manifesto, diametralmente oposto à aprovação do projeto (GOOGLE..., 2023). O teor da manifestação não possuía indicativos sobre qual viria a ser a problemática causada pela legislação, mas tão somente que resultados e efeitos negativos ocorreriam, em direção totalmente oposta à própria proposta da lei. A plataforma de comunicação Telegram, no mesmo sentido, enviou a seus usuários mensagens de solicitação de apoio e manifestação contra a aprovação do referido projeto de lei (PL..., 2023).

Pela quantidade de acontecimentos no ano de 2023, especialmente de manifestações – a favor e contra – o PL das *fake news*, entende-se que o enfrentamento da temática demandaria um trabalho inteiro, de modo que esta monografia faz a mera menção ao projeto e às repercussões por ele geradas. Salienta-se, no entanto, que se torna visível, ao observar o caso, que empresas de

[14] O projeto se popularizou com o nome de PL das *fake news*.

tecnologia, diante da possibilidade de diminuição do seu poder de alcance/atuação, lançam mão de todos os meios possíveis para evitar qualquer mitigação.

Em seu livro, Shoshana Zuboff propõe diretrizes a serem observadas pela legislação para regular o fenômeno do capitalismo de vigilância, e, por conseguinte, assegurar efetiva proteção aos utilizadores:

> Precisamos de leis que rejeitem a legitimidade fundamental das declarações do capitalismo de vigilância e interrompam suas operações mais básicas, inclusive a renderização ilegítima da experiência humana como dados comportamentais; o uso de superávit comportamental como matéria-prima gratuita; as concentrações extremas dos novos meios de produção; a fabricação de produtos de predição; os negócios em futuros comportamentais; o uso de produtos de predição para operações de modificação, influência e controle de terceiros; as operações dos meios de modificação comportamental; a acumulação de concentrações exclusivas privadas de conhecimento (o texto sombra); e o poder que tais concentrações conferem. (ZUBOFF, 2020, p.i.)

Com base nas colocações da autora, a fim de rejeitar a legitimidade e interromper as operações ilegítimas mais básicas, o ordenamento jurídico deverá reconhecer, em primeiro lugar, o cenário de capitalismo de vigilância. Assim reconhecido, será possível o encaminhamento e a regulação do fenômeno, assegurando segurança aos dados dos usuários, a efetivação da autodeterminação informativa, atualmente positivada no Brasil, como veremos a partir de agora.

3 A PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO BRASILEIRO

Antes de iniciar o enfrentamento da matéria de proteção dos dados pessoais, é pertinente tecer algumas considerações sobre o panorama legislativo da matéria. Os trabalhos de Doneda (2011), Martins e Tateoki (2019) e Lugati e Almeida (2020) revisitam a classificação legislativa proposta por Viktor Mayer-Schönberg. Segundo tal classificação, fala-se na existência de quatro gerações de leis de proteção de dados pessoais, as quais serão abordadas brevemente.

A primeira geração, datada da década de 1970, possui enfoque na concessão de autorização para que o Estado constitua bancos de dados dos cidadãos, com ênfase no controle e no uso das informações obtidas. É possível dizer que a privacidade, nesta geração, está relegada ao segundo plano. A segunda geração passa a levar em conta a efetividade do consentimento do titular dos dados, bem como a liberdade para não os disponibilizar. Assim, percebe-se aumento na autonomia do

usuário. Por sua vez, a terceira geração, datada da década de 1980, é marcada por legislações que visam à efetividade dos direitos de privacidade, e começa a surgir o conceito de autodeterminação informativa, enfrentado adiante. No entanto, o enfoque é ainda mais individualizado, isto é, voltado ao utilizador. A quarta e atual geração prioriza o titular dos dados em relação a terceiros. Eleva-se, nesta geração, o padrão coletivo de proteção dos dados. Muito embora os autores acima indicados tenham trazido exemplos de legislações internacionais para ilustrar cada uma das legislações, este trabalho deixa de mencioná-las propositalmente, pois a estrutura desta monografia não comporta o enfrentamento do direito comparado, o que demandaria trabalho com maior fôlego.

As temáticas enfrentadas nos próximos subcapítulos estão intimamente ligadas entre si. A divisão dos subcapítulos foi definida tanto pelo binômio infraconstitucional e constitucional, e a ordem de construção, pelo fator temporal. As legislações infraconstitucionais entraram em vigor antes da jurisprudência do Supremo Tribunal Federal e promulgação da Emenda Constitucional n. 115/2022. Aliás, estes dois últimos são influenciados diretamente por aqueles, de modo que se faz necessário enfrentar e compreender a legislação infraconstitucional para, então, adentrar às razões de decidir do STF e debates que levaram à promulgação da EC n. 115/2022.

3.1 A LEGISLAÇÃO BRASILEIRA: O MARCO CIVIL DA INTERNET, A LGPD E A (DES)PROTEÇÃO DE DADOS PESSOAIS NO NÍVEL INFRACONSTITUCIONAL

Inicialmente, uma ressalva se faz necessária. Não se desconhece que a legislação brasileira encontra previsões sobre dados pessoais no Código de Defesa do Consumidor (Lei n. 8.078/1990), na Lei de Acesso à Informação (Lei n. 12.527/2011), na lei que tipifica os delitos informáticos (Lei n. 12.737/2012) e na Lei do Governo Digital (Lei n. 14.129/2021). Porém, tais legislações não abordam a temática dos dados pessoais no contexto de sociedade da informação. Em verdade, o Código de Defesa do Consumidor (BRASIL, 1990) dispõe sobre os bancos de dados dos consumidores relacionados ao consumo e ao crédito, bem como prevê o direito de o consumidor ter acesso aos dados relativos a si. Por sua vez, a Lei de Acesso à Informação (BRASIL, 2011), muito embora disponha sobre informações pessoais, remete-se à proteção conferida pelos termos da Lei Geral de Proteção de dados, que será enfrentada adiante. Da mesma forma, a Lei do Governo Digital (BRASIL, 2021)

também dispõe brevemente sobre o direito do cidadão à proteção dos dados e remete-se à proteção conferida pela LGPD. Por fim, a lei que tipifica os delitos telemáticos (BRASIL, 2012) versa sobre condutas voltadas à quebra da segurança de dispositivos por outras pessoas, não havendo falar-se em correlação com o capitalismo de vigilância. Em verdade, como referido linhas acima, as posturas das gigantes da tecnologia possuem uma aura de legitimidade em razão dos termos de uso, não guardando relação alguma com o tipo penal da lei suprarreferida. Não é demais ressaltar que breves considerações ao Projeto de Lei n. 2.630/2020 (PL das *fake news*) já foram realizadas no capítulo anterior por não se tratar de norma vigente no ordenamento brasileiro.

Borges (2021) enfrenta parte das legislações acima referidas, pontuando as disposições acerca dos dados e da privacidade do titular. A autora, diante das disposições das legislações anteriores, assevera a importância e a necessidade da existência da Lei Geral de Proteção de Dados. Assim sendo, esta monografia se limita ao enfrentamento, na seara infraconstitucional, às previsões do Marco Civil da Internet (Lei n. 12.965/2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), os quais serão trabalhados a partir de agora.

O Marco Civil da Internet (doravante apenas “Marco Civil”) foi sancionado no ano de 2014, com o objetivo de regular o uso da internet no Brasil. Sem prejuízo das demais disposições, o Marco Civil possui, no que toca diretamente a este trabalho, a proteção da privacidade e a proteção dos dados pessoais como princípios norteadores (art. 3º, II e III). Ainda, o art. 6º orienta a interpretação da norma no sentido da natureza da internet, os usos e costumes e a importância da rede para o desenvolvimento humano, econômico, social e cultural. Por sua vez, o Capítulo II (arts. 7º e 8º) prescreve os direitos dos usuários ao utilizarem a rede mundial de computadores.

As previsões do art. 7º são especialmente caras a esta monografia, pois, em um cenário de capitalismo de vigilância e captura de superávit comportamental, os incisos VII e VIII se mostram um tanto problemáticos:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser

> utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. (BRASIL, 2014, p.i.) (sem omissões no. original)

Em primeiro lugar, o inciso VII assegura a privacidade dos dados do utilizador, facultando, porém, o fornecimento a terceiros nos casos de consentimento livre, expresso e informado. O trabalho de Barreto Junior, Sampaio e Gallinaro (2018) se debruçou sobre a temática da privacidade em relação ao Marco Civil. No entanto, a perspectiva não é animadora. O consentimento se mostra uma figura problemática na legislação. Os autores argumentam que, no contexto da Sociedade da Informação, existem produtos e serviços indispensáveis, como, por exemplo, um serviço de *e-mail* destinado às atividades laborativas do utilizador. Nesse sentido, em existindo dependência do serviço – em clara evidência da assimetria existente entre o usuário e o provedor –, o utilizador se vê sem alternativa que não a aceitação dos termos. Mendes e Fonseca (2020) igualmente se debruçam sobre a temática do consentimento, e concluem que o instituto, apesar de basilar, não possui os efeitos esperados na seara da proteção dos dados pessoais. Esse artigo também fornece perspectivas contemporâneas de materialização e efetivação dos direitos dos usuários em rede, as quais serão trabalhadas após as reflexões sobre as disposições da LGPD.

Em segundo lugar, o inciso VIII garante ao usuário informações claras sobre a coleta, armazenamento e tratamento de seus dados. No entanto, apoiando-nos na teorização do capitalismo de vigilância por Zuboff, especialmente nas práticas obscuras e no ciclo de despossessão, o panorama de efetividade da legislação é igualmente desanimador. Com efeito, se as maiores descobertas sobre as práticas das gigantes da tecnologia ocorreram por meio de vazamentos e investigações, sem qualquer transparência por parte das instituições, não se pode presumir – quiçá esperar – a obtenção de informações claras e completas. Da mesma forma, dada a tendência de buscar acobertar os feitos, protelá-los, ou, em último caso, realizar alterações superficiais, não se afigura possível, em um contexto de capitalismo de vigilância, que a norma seja efetiva.

Ao fim e ao cabo, o trabalho de Barreto Junior, Sampaio e Gallinaro (2018) sinaliza que, por se tratar de uma “lei diretiva, que consubstancia o ânimo legislativo

de um país" (BARRETO JUNIOR, SAMPAIO, GALLINARO, 2018, p.118), e, por conseguinte, garantidora de direitos, é possível depreender a natureza de direito fundamental das previsões do Marco Civil, pois os direitos nele previstos são reafirmações dos direitos constitucionais à privacidade e à intimidade.

Tomasevicius Filho (2016) teceu várias críticas ao Marco Civil, as quais extrapolam o contexto de capitalismo de vigilância. Em tom mais ácido, o autor assevera que a lei, primeira no mundo a regular o uso da internet, era objeto de ingenuidade do legislador, que intentava "manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional" (TOMASEVICIUS FILHO, 2016, p. 276). Apesar disso, o autor pontua existirem três pontos positivos: a vedação da imposição de mecanismos de censura, bloqueio, monitoramento e filtragem, na forma do art. 9º, §3º; a regulamentação dos procedimentos judiciais específicos para obtenção de dados de navegação para fins de instrução processual civil e penal; e a disciplina dos *cookies*, definidos pelo autor como os "arquivos instalados nos computadores ou telefones para registrar informações e preferências dos usuários quando acessam determinada página na internet" (TOMASEVICIUS FILHO, 2016, p. 278)[15]. Ainda assim, o autor arremata que, em sendo de caráter extraterritorial, uma legislação nacional não se faz suficiente aos desafios trazidos pela internet, entendendo necessária a elaboração de norma jurídica internacional, como uma Lei Uniforme ou Convenção Internacional sobre o uso da internet, a fim de unificar o tratamento dispensado aos atores envolvidos na rede. Dado o ano do trabalho, não era possível antever o desfecho do cenário internacional, porém, anos depois, entrou em vigor o Regulamento Geral de Proteção de Dados (GDPR, na sigla original), aplicável a todas as pessoas físicas e jurídicas da União Europeia e Espaço Econômico Europeu. O Regulamento foi fonte inspiradora da Lei Geral de Proteção de Dados (LGPD), sobre a qual trataremos agora.

Sancionada em 2018 e totalmente em vigor em 2020, a Lei n. 13.709/2018 foi oriunda dos Projetos de Lei n. 4.060/2012 e 5.276/2016. Este projeto foi enfrentado por Menezes Neto, Morais e Bezerra (2017). Em seu trabalho, ao contextualizarem o contexto de *dataveillance* que se desdobra em capitalismo de vigilância, os autores

[15] Quanto a este caso, ressalva-se que o consentimento quanto aos *cookies* também redunda na problemática do consentimento em geral, de modo que, em um cenário de capitalismo de vigilância, não é possível falar com certeza em "avanço" da legislação ao dispor sobre a necessidade de consentir com a captura dos dados por meio dos *cookies*.

alertam não ser mais possível falar em tratamento diferente para categorias de dados diferentes, pois dados são apenas dados. Não no sentido do conteúdo desses dados, mas em relação a sua categoria, especialmente os anônimos, porquanto os dados anonimizados são facilmente revertidos e o titular logo é localizado. Os autores expõem casos em que foi possível a reversão do processo de anonimização, e concluem, em relação às previsões do Projeto de Lei que a legislação, apesar de inovadora e essencial, limita-se a dados pessoais, sem trazer mecanismos efetivadores de igualdade:

> verificou-se que, embora importantes, os mecanismos de controle estatais (como PL 5276/2016, para a proteção dos dados pessoais no Brasil) são incapazes de proteger, adequadamente, os direitos humanos, o que ocorre como consequência de alguns fenômenos: da globalização; do surgimento de novos centros de poder não estatais; e da expansão das tecnologias da informação. Todos eles possuem, em comum, a extrema facilidade para transpor espaços físicos — o foi referido através das ideias de desterritorialidade e desespacialidade.
> Uma das consequências fundamentais derivada da matriz teórica dos *surveillance studies* é a superação da ideia de que informações pessoais e comunicações privadas dizem respeito apenas às violações da privacidade. Esse lugar-comum no direito, resultado da não compreensão da categoria da surveillance, faz com que os juristas já comecem a encarar o problema de maneira equivocada, conforme foi demonstrado pela ausência do enfrentamento — pelo PL 5276/2016 — das cruéis violações da igualdade e da liberdade patrocinadas pela tecnologia da informação.
> [...]
> Por isso, é possível — e necessário — compreender que as TICs atingem muito mais que a privacidade, podendo servir como um instrumento de segregação social e caracterizador da violação à isonomia e à dignidade. São insuficientes as tentativas de restringir os fluxos de dados na sociedade em rede por meio de mecanismos rígidos, centrados em territórios, como é o caso das legislações derivadas do Estado-nação. (MENEZES NETO, MORAIS, BEZERRA, 2017, p. 196-7) (sem omissões no original)

O trabalho permite inferir que uma legislação efetiva deve ultrapassar o âmbito dos dados – pessoais, sensíveis ou anônimos –, reconhecendo o contexto de capitalismo de vigilância como causa, para, então regulá-lo. Essa conclusão vai no mesmo sentido da teorização de Zuboff.

Após publicada, a LGPD foi objeto de estudo em inúmeros trabalhos. A legislação inicia, em seu art. 1º, expondo possuir “o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018, p.i.). Na sequência, o legislador expõe os fundamentos da legislação (art. 2º), dentre os quais, sem prejuízo dos demais, vale a menção à autodeterminação informativa (inciso II). Inaugurada na

legislação brasileira na LGPD, a autodeterminação informativa já foi reconhecida na década de 1980 na Alemanha, consoante o trabalho de Mendes (2020). O trabalho aponta, ainda, que esse fundamento pode ser visualizado como um desdobramento dos direitos de personalidade, surgido para adequar a necessária proteção do indivíduo no contexto da era da informação. Em síntese, a autodeterminação informativa pode ser entendida como o direito que o titular de dados possui de conhecê-los, controlá-los e protegê-los. Outro fundamento que salta aos olhos é a liberdade de expressão, informação, comunicação e opinião (inciso III). No mesmo sentido do trabalho desenvolvido por Tomasevicius Filho (2016) sobre o Marco Civil, é possível depreender que o legislador, influenciado pelos resquícios do período ditatorial, preocupou-se em não deixar margem a qualquer possibilidade de censura ao inserir este fundamento na Lei Geral de Proteção de Dados.

A legislação apresenta, em seu art. 5º, a conceituação de termos correlatos aos dados pessoais. Para os fins deste trabalho, faz-se necessária a revisitação de alguns conceitos, a saber: dado pessoal (inciso I), dado pessoal sensível (inciso II), dado anonimizado (inciso III), titular (inciso V), controlador (inciso VI), operador (inciso VII), tratamento (inciso X), anonimização (inciso XI) e consentimento (inciso XII). Sem prejuízo das demais, essas definições são especialmente caras a esta monografia por estarem intimamente ligadas à relação existente entre o usuário (titular dos dados pessoais) e as gigantes da tecnologia, e, por conseguinte, com o próprio capitalismo de vigilância. Em primeiro lugar, dado pessoal é toda a informação relacionada a alguma pessoa natural identificada ou identificável. Por sua vez, o dado pessoal sensível é a informação “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, 2019, p.i.). O último tipo de dado elencado na LGPD é o dado anonimizado, assim entendidas as informações relativas ao titular, que não sejam passíveis de identificação, “considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (BRASIL, 2019, p.i.). De forma breve, titular é o usuário que gera dados sobre si durante a navegação, controlador é a pessoa natural ou jurídica responsável pelo tratamento de dados, e operador é a pessoa natural ou jurídica que realiza o tratamento de dados a mando do controlador. A seu turno, nos termos da LGPD, tratamento é

> 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. (BRASIL, 2019, p.i.)

Por fim, a anonimização consiste em processo que impossibilita a associação de um dado a seu titular, e consentimento é definido como a manifestação livre, informada e inequívoca de concordância do titular com o tratamento de seus dados para uma finalidade imediata.

Como já referido anteriormente, o consentimento é uma figura problemática no contexto de capitalismo de vigilância. As considerações referentes ao consentimento no Marco Civil se repetem em certa medida em relação à LGPD. Muito embora a conceituação agora se volte a uma manifestação livre, informada e inequívoca, ainda são encontrados resquícios de um consentimento não muito livre, pouco informado, e, em casos extremos, equivocado. Fornasier e Knebel (2021), partindo de uma visão materialista do capitalismo de vigilância – em que os dados seriam a mais valia do usuário –, discorrem sobre o consentimento na LGPD enquanto instituto impraticável. Os autores contextualizam a necessidade de utilização de determinados produtos/serviços das TICs, o que tensiona o utilizador a se sujeitar aos termos de uso. Dessa forma, em que pese o utilizador tenha consentido com o tratamento de seus dados, o consentimento fornecido não corresponde ao previsto na legislação, haja vista não preencher os requisitos de liberdade, informação e certeza/inteligibilidade. Os autores concluem que a legislação deve enfrentar o consentimento levando em conta o contexto de mercantilização de dados e o próprio capitalismo de vigilância que o permeia.

De mais a mais, a LGPD é marcada por possuir grande carga principiológica. O art. 6º prevê, para além da boa-fé, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, e responsabilização e prestação de contas, nos incisos I ao X, respectivamente. O trabalho construído por Santos (2021), lançando mão pontualmente do direito comparado, sinaliza que a legislação possui fortes relações com o Direito europeu, especialmente em relação ao Regulamento Geral de Proteção de Dados (RGPD). Ainda, a autora aponta existir uma tendência internacional de constitucionalização do direito à proteção dos dados pessoais, sendo um dos reflexos desse cenário a Proposta de Emenda à Constituição (PEC) n. 17/2019, a qual

culminou na Emenda Constitucional (EC) n. 115/2022, enfrentada no subcapítulo seguinte. O trabalho ainda indica uma forma de cisão da proteção dos dados pessoais em relação ao direito à privacidade. Com efeito, a proteção aos dados pessoais passa a ser direito autônomo e independente, não sendo mais necessária sua correlação direta com a privacidade.

No entanto, apesar de ser considerada um marco jurídico no ordenamento brasileiro, consoante o trabalho de Fornasier e Knebel (2021), a LGPD padece de uma ambiguidade. Segundo os autores, muito embora a legislação preveja a (hiper)vulnerabilidade do usuário, existe a faculdade do utilizador em ceder seus dados para tratamento. Se, de um lado, o utilizador é figura vulnerável em relação ao controlador e operador, do outro, o utilizador é livre para ceder seus dados. É possível depreender que essa ambiguidade afasta a legislação do diálogo necessário com o capitalismo de vigilância teorizado por Zuboff.

Para além dessa ambiguidade, Morellato e Santos (2021) enfrentam o inciso V do art. 7º da LGPD[16]. Para os pesquisadores, a disposição é um tanto aberta, norteada pelos princípios elencados anteriormente. No entanto, apontam os autores que a disposição tal qual foi positivada pode esvaziar toda a proteção prevista na lei, especialmente se considerarmos o histórico das *big techs*. Segundo os autores, a redação do inciso V

> permite que o simples fato de constar do contrato uma cláusula que assegura ao fornecedor o poder de coleta dos dados o isenta da obrigatoriedade de consentimento livre, informado e inequívoco do usuário da plataforma ou outro consumidor em geral. (MORELLATO; SANTOS, 2021, p. 196)

Os pesquisadores também enfrentam a temática do legítimo interesse, prevista no inciso IX do art. 7º[17].

Com efeito, ficou evidenciado que (se não toda, então) a maciça maioria das violações perpetrada por meio de alguma TIC já vinha prevista nos termos de uso.

---

[16] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[...]
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. (BRASIL, 2018, p.i.)

[17] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[...]
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 (BRASIL, 2018, p.i.) (sem omissões no original)

Sobre tal violação já existia consentimento prévio do utilizador em algum momento, mesmo que não fosse possível depreender dos termos do contrato. A captação e tratamento dos dados já vem formalmente autorizada em algum trecho, muito embora isso implique reflexos negativos ao usuário. Ao fim e ao cabo, os autores apostam na instituição do legítimo interesse enquanto norteador da aplicação do tratamento de dados. No entanto, o instituto ainda carece de balizas para a aplicação no caso concreto.

Camurça e Matias (2021) retomam a problemática da anonimização de dados na LGPD, mas com enfoque na publicidade direcionada. Após revisitarem a problemática do consentimento (ou "pseudoconsentimento"), os autores discorrem sobre a captação de *cookies*, *supercookies* e *fingerprinting*, e como essas técnicas fragilizam os dados anônimos. Os autores apontam que a técnica de *fingerprinting*, quando empregada com o auxílio da inteligência de máquina, pode não apenas reverter o processo de anonimização dos dados, mas também obter informações mais precisas sobre o perfil do usuário do que aquelas efetivamente prestadas pelo utilizador. Os autores refletem que a publicidade direcionada não é um problema em si. Em verdade, na visão dos pesquisadores, a maior preocupação deve se voltar em relação às práticas obscuras empregadas pelas empresas de tecnologia no tratamento dos dados dos usuários.

De outra parte, em sua tese de doutoramento, Queiroz (2021) enfrenta a temática da Autoridade Nacional de Proteção de Dados (ANPD), instituída pela LGPD. A autora contextualiza a figura do Encarregado, prevista no art. 5, VIII, da lei suprarreferida. Essa pessoa, escolhida pelo controlador realizará a comunicação entre ele e a ANPD. A autora aborda criticamente as atribuições e a ausência de regulamentação da responsabilidade civil do encarregado. Segundo a autora, o encarregado, para além da comunicação, zelará pela proteção dos dados dos usuários dentro do serviço/produto oferecido pelo controlador. Todavia, considerando-se o histórico de obscuridade praticado pelas empresas de tecnologia – especialmente as cinco grandes –, e considerando que o encarregado será indicado pelo controlador, talvez não seja possível vislumbrar efetiva proteção dos dados pessoais dos usuários. Ao final, Queiroz propõe uma lista das atribuições entendidas necessárias ao exercício da função de encarregado, o qual deverá estar em contato próximo com o mais alto nível de gestão, bem como deverá possuir amplo conhecimento técnico. Sugere, ainda, que a responsabilidade civil atribuída ao encarregado seja a subjetiva. Sobre a

mesma temática, o trabalho de Andrade e Barreto (2020) enfrentou a vinculação da ANPD à Presidência da República. Os autores defendem a necessidade de instituição de uma ANPD autônoma e independente, para atingir totalmente seus objetivos. Do contrário, argumentam os pesquisadores que a ausência de independência pode ocasionar em infrações que passem despercebidas.

Apesar de Queiroz (2021) defender que a nova conformação e a atuação do encarregado sedimentem uma cultura de proteção de dados pessoais nas empresas, e, por conseguinte, seus produtos e serviços, não se pode afirmar com certeza a concretização dessa cultura. Em verdade, somente estudos posteriores, realizados a longo prazo, poderão trazer conclusões nesse sentido.

Em suma, muito embora a LGPD seja importantíssima à proteção de dados pessoais no ordenamento jurídico brasileiro, é possível depreender que a norma não reconhece o capitalismo de vigilância que a permeia. Apesar de prescrever princípios e direitos de proteção aos titulares, a norma não busca regular o fenômeno em si, o que pode ocasionar a manutenção das violações já existentes. Como já referido anteriormente, à luz da indiferença radical e em havendo retorno em pecúnia, persiste o interesse dos capitalistas de vigilância no tratamento dos dados pessoais sem a observância dos princípios insculpidos no art. 6º da Lei Geral de Proteção de Dados. Com isso, infere-se que não basta a previsão de proteção e eventuais sanções ao uso indevido/discriminatório, se não houver algum mecanismo legal capaz de frear o fenômeno que orienta o tratamento de dados.

Para fazermos uso da alegoria trazida por Zuboff, o ordenamento jurídico deve estar preparado para lidar não apenas com as marionetes, mas também – e, ousa-se dizer, principalmente – com o titeriteiro. Assim, por meio de uma regulação efetiva do capitalismo de vigilância (voltando-se o sistema a um capitalismo da informação, consoante teorizado por Zuboff), violações e discriminações poderão ter fim, assegurando um ambiente *on-line* mais sadio e seguro aos usuários e seus dados.

De toda sorte, mesmo que o enfrentamento da legislação infraconstitucional tenha promovido uma perspectiva de proteção tímida e um tanto ineficiente, mesmo que inovadora no ordenamento, passa-se ao enfrentamento da jurisprudência já existente do Supremo Tribunal Federal, a Emenda Constitucional n. 115/2022, e quais perspectivas poderão ser esperadas do patamar de direito fundamental atribuído à proteção dos dados pessoais.

3.2 A JURISPRUDÊNCIA DO SUPREMO TRIBUNAL FEDERAL E A EC N. 115: A PROTEÇÃO DE DADOS COMO DIREITO FUNDAMENTAL

Neste último subcapítulo, esta monografia se debruça, em um primeiro momento, sobre o julgamento conjunto das ADIs n. 6387, 6388, 6388, 6389, 6390 e 6393. Na sequência, será enfrentada a Emenda Constitucional n. 115/2022.

No ano de 2020, com o advento da pandemia de COVID-19, causada pelo vírus SARS-CoV-2, a Presidência da República editou a Medida Provisória n. 954/2020. Em síntese, a Medida permitia o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística – IBGE (BRASIL, 2020).

Pouco tempo depois, o Supremo Tribunal Federal (STF) foi provocado por meio de Ações Diretas de Inconstitucionalidade (ADIs), para o fim de declarar a inconstitucionalidade da medida. As ações, todas impugnando a constitucionalidade da MP n. 954/2020, foram autuadas com os números 6387, 6388, 6389, 6390 e 6393. Os Ministros, por maioria, decidiram que a referida MP não possuía interesse público legítimo para captar e tratar dados, tampouco apresentou mecanismo técnico capaz de proteger os dados de eventuais acessos não autorizados, vazamentos acidentais ou utilização indevida no tratamento. O julgamento do pleito liminar pelo STF foi considerado histórico, pois a Corte reconhecera, pela primeira vez, o caráter de direito fundamental da proteção dos dados pessoais (STF, 2020). Faz-se válida a colação da ementa do julgamento:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O

> compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam “adequados, relevantes e não excessivos em relação a esse propósito” e “conservados apenas pelo tempo necessário.” (artigo 45, § 2º, alíneas “b” e “d”). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (BRASIL, 2020)

Apesar de não haver menção expressa na ementa, os Ministros enfrentaram a constitucionalidade da proteção dos dados pessoais. Em seu voto, o Ministro Luiz Fux discorreu sobre a natureza constitucional da proteção de dados pessoais e a autodeterminação informativa, tratando-se de direitos fundamentais autônomos. O Ministro, em relação ao caso apreciado, apontou existir enorme desproporcionalidade entre a generalidade das prescrições da norma e o volume e importância dos dados compartilhados.

O Ministro Ricardo Lewandowski, após ressaltar a importância da instituição

IBGE para a elaboração de políticas públicas, ponderou que a disponibilização de tais dados, sem o devido aporte protecional, possuía grandes chances de implicar uso desvirtuado das informações obtidas, causando desassossego aos titulares.

Acompanhando a relatora, o Ministro Gilmar Mendes discorreu sobre imprescindibilidade e inevitabilidade da tecnologia na humanidade. Criticou, contudo, usos que se desdobram em discriminações por parte dos algoritmos, citando como exemplo a utilização de inteligência artificial para fornecimento de hospitalização a pacientes com base em critérios como probabilidade de sobrevivência e qualidade de vida no pós-tratamento.

O Ministro Luís Roberto Barroso apontou tratar-se de caso de ponderação entre a estatística – e sua característica de ferramenta indispensável ao mundo contemporâneo –, e o direito à privacidade.

Apenas o Ministro Marco Aurélio proferiu voto divergente. O Ministro ressaltou a importância da manutenção dos serviços realizados pelo IBGE, bem como a preponderância do interesse público sobre o interesse particular. Dessa forma, o Magistrado entendeu tratar-se do interesse do particular em não ver compartilhados os seus dados contra o interesse público nos serviços prestados pelo IBGE, cuja importância é indiscutível, especialmente ao desenvolvimento de políticas públicas. Em sua fundamentação, entendeu que o aspecto coletivo deve preponderar em relação ao interesse privado, ainda mais considerando tratar-se a medida provisória da confiança de dados sensíveis a uma instituição conhecida e respeitada no Brasil.

Ao final, as ADIs foram extintas sem resolução do mérito, em razão da perda superveniente do objeto, uma vez que o prazo de vigência se encerrou no dia 14 de agosto de 2020, enquanto os processos ainda tramitavam. No entanto, mesmo se tratando do julgamento pelo Tribunal Pleno de pleito liminar, o Supremo deixou evidente o entendimento segundo o qual o direito à proteção dos dados pessoais possui força constitucional. Seja um direito fundamental autônomo, ou um direito fundamental enquanto desdobramento dos direitos fundamentais à privacidade e ao sigilo das comunicações, a proteção de dados pessoais foi considerada um direito fundamental por todos os ministros favoráveis ao deferimento do pedido liminar. É importante ressaltar que, à época, a LGPD ainda se encontrava em *vacatio legis*, porém suas disposições já foram levadas em consideração pelos julgadores.

Desse julgamento, para além do reconhecimento da natureza de direito fundamental da proteção dos dados pessoais, foi possível colher esse princípio

enquanto desdobramento da dignidade da pessoa humana, bem como da autodeterminação informativa, de maneira um tanto desvencilhada da privacidade, como até então veio sustentado. Como será visto adiante, esse entendimento dissociado fez parte da compreensão do legislador ao elaborar a Emenda Constitucional n. 115/2022.

Jalil e Burlamaqui (2022), ao enfrentar o reconhecimento da proteção de dados como direito fundamental, sinalizam que o contexto de capitalismo de vigilância e a grande disparidade existente entre o utilizador e o controlado devem ser levados amplamente em conta:

> A declaração da proteção de dados como direito autônomo e fundamental decorre, assim, da inafastável necessidade da afirmação dos direitos fundamentais e de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional. Os espaços digitais são controlados por agentes econômicos com alta capacidade de coleta, armazenamento e processamento de dados pessoais com intenso fluxo na internet colocando em alto risco a possibilidade de violação dos direitos de personalidade e privacidade, por se tratar de um cenário hipervulnerável, cujos traços de vulneração são peculiares e se sobrepõem ao ordinário daí decorrendo a afirmação da proteção de dados como direito fundamental. (JALIL; BURLAMAQUI, 2022, p. 11)

Queiroz (2021) discorre sobre a positivação implícita da proteção dos direitos fundamentais a partir da interrelação com os demais princípios constitucionais:

> Vale lembrar que outros direitos fundamentais elencados no rol do art. 5º fazem conexão com o direito à proteção de dados pessoais, como a intimidade, a vida privada, a honra, a imagem e o sigilo das comunicações de dados.
> Além deles, destaca-se o livre desenvolvimento da personalidade, fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados. A partir dele e da leitura harmônica e sistemática da Constituição Federal, é possível concluir que está implicitamente positivado o direito fundamental à proteção de dados pessoais. (QUEIROZ, 2021, p. 38)

Mesmo já sendo considerada direito fundamental pelo Supremo, Queiroz (2021, p. 19) aponta que a previsão de proteção conferida pela Constituição até então não era suficiente. Muito embora fosse possível o manejo dos institutos jurídicos, em um país como o Brasil, que possui problemas estruturais de maior gravidade, a proteção de dados pessoais era uma questão de menor apelo. Ademais, muito embora se tratasse de direito implícito no texto constitucional em razão da proteção da privacidade e inviolabilidade de comunicação, a ausência de previsão expressa

também poderia implicar certa permissividade quanto à utilização dos dados dos usuários (QUEIROZ, 2021, pp. 37-8).

Foi sob esse parâmetro que teve início a tramitação da Proposta de Emenda à Constituição (PEC) n. 17/2019, de origem do Senado Federal. O então Senador e autor Eduardo Gomes, no corpo da justificação, afirmou que a constitucionalização da proteção dos dados pessoais é medida de bom alvitre, citando países como Portugal, Estônia, Polônia e Chile, que atribuíram valor constitucional à temática.

No dia 22 de maio de 2019, sobreveio parecer favorável da Comissão de Constituição de Justiça (BRASIL, 2019). O parecer, cuja relatoria coube à então senadora Simone Tebet, apontou não existir causa circunstancial capaz de macular a constitucionalidade da PEC. O documento levou em conta tendências internacionais de elaboração legislativa no sentido de garantir a proteção dos dados pessoais. Ainda, assim dispõe o parecer:

> pode-se afirmar que, questões efetivas e atuais como a eficácia horizontal dos direitos fundamentais, a proteção dos direitos da personalidade, principalmente a proteção à privacidade e intimidade, o direito ao esquecimento como atributo relativo ao direito da personalidade, trazem à baila a necessidade da proteção dos dados pessoais com enfoque constitucional.
> [...]
> Assim, a PEC no 17, de 2019, ao inserir a proteção dos dados pessoais no rol das garantias individuais - ao lado de direitos fundamentais consagrados - garante, ainda, a certeza jurídica que se faz premente em uma sociedade abarcada por conflitos sociodigitais e por uma legislação ainda incipiente sobre o tema. (BRASIL, 2019, pp. 6-7) (Sem omissões no original)

Após o Parecer, o texto proposto pelo Senado alteraria o art. 5º, XII, da Constituição Federal, a fim de incluir a proteção aos dados pessoais junto às disposições sobre inviolabilidade de correspondência.

Remetida a Proposta ao Senado, o Deputado João Roma expediu parecer favorável à admissibilidade da PEC.

Nos meses de maio, novembro e dezembro de 2021, o Senado Federal recebeu cinco manifestações de diversas instituições que, em conjunto e em uníssono, manifestaram apoio à PEC, e solicitaram o trâmite preferencial.

Em 4 de dezembro de 2019, sobreveio parecer do Deputado Orlando Silva, relator da PEC na Câmara dos Deputados, manifestando-se pela inclusão de um novo

inciso (a saber, o inciso LXXIX[18]) ao invés da alteração do inciso XII (BRASIL, 2019). Em sua fundamentação, o relator apontou, após levar em consideração as audiências públicas então realizadas, que a privacidade veiculada no inciso XII possui cunho individual, enquanto que a proteção dos dados pessoais é matéria de cunho coletivo. Daí falar-se em um novo inciso. Para mais, o próprio conceito de proteção dos dados pessoais diverge do conceito de privacidade e inviolabilidade telemática, de modo que a temática adquiriu autonomia suficiente, pelo que se fez necessária a inclusão de um novo dispositivo. Além da positivação da proteção dos dados pessoais como direito fundamental expresso, a PEC também alterou o art. 22 do texto constitucional, para atribuir à União a competência exclusiva para legislar sobre a matéria[19].

Doneda (2011) discorre sobre o caráter de direito fundamental da proteção dos dados pessoais. No mesmo sentido do trabalho de Queiroz e do parecer do Deputado Orlando Silva, o autor defende que a constitucionalização da temática é medida adequada, pois existe um hiato entre o direito à privacidade e a proteção das informações, de modo que é possível a violação da privacidade – ou qualquer outro direito fundamental – por meio da violação da proteção dos dados pessoais. O trabalho trouxe, ainda, decisão exemplificativa do STF. Sob relatoria do Ministro Sepúlveda Pertence, a decisão "reconheceu expressamente a inexistência de uma garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais, endossando tese de Tércio Sampaio Ferraz Júnior, segundo a qual o ordenamento brasileiro tutelaria o sigilo das comunicações – e não dos dados em si". (DONEDA, 2011, p. 105)

A previsão expressa da proteção de dados pessoais como direito fundamental na constituição se traduz, com base nos trabalhos elencados acima, no acompanhamento do ordenamento jurídico brasileiro em relação aos "avanços" tecnológicos. No entanto, para os fins deste trabalho, o ordenamento – e, em especial, o *novel* inciso LXXIX do art. 5º da CF/88 – deve ser enfrentado sob a ótica do capitalismo de vigilância.

Em considerando as direções indicadas por Zuboff sobre como deve ser construída uma legislação efetiva de proteção de dados, pontuada anteriormente, é

[18] LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (BRASIL, 1988, p.i.)

[19] Art. 22. Compete privativamente à União legislar sobre:
[...]
XXX - proteção e tratamento de dados pessoais. (BRASIL, 1988, p.i.) (sem omissões no original)

possível depreender que o ordenamento jurídico brasileiro não possui proteção efetiva, pois não reconhece, ao fim e ao cabo, o contexto do capitalismo de vigilância. A medida é necessária para a regulação do fenômeno, e, via de consequência, o encaminhamento a uma sociedade mais segura, em que sejam respeitados os dados dos usuários, bem como sua autodeterminação informativa.

Nesse sentido, o principal resultado deste trabalho possui um panorama um tanto pessimista: o ordenamento jurídico brasileiro não é suficiente à regulação do fenômeno do capitalismo de vigilância, de modo que a proteção dos dados pessoais e a autodeterminação informativa dos utilizadores das TICs ainda se encontra vulnerabilizada. Violações ainda continuarão a ocorrer, porque as medidas adotadas no âmbito jurídico atuam – para relembrar a alegoria de Zuboff – tão somente sobre as marionetes, sem tocar o titeriteiro. Assim, uma perspectiva possível é a do surgimento de novas marionetes, o que é inevitável, mas com a manutenção da dinâmica já explicitada.

Mesmo assim, é importante ressaltar que esse cenário não é uma exclusividade brasileira. Em verdade, as medidas trabalhadas nesta monografia sinalizam que o Brasil vem mantendo o passo com inovações legislativas e jurisprudenciais de nível avançado em todo o mundo. Para mais, com o *status* de direito fundamental atribuído à proteção dos dados pessoais, apesar da abstração da previsão constitucional, o legislador orienta a aplicação da norma ao melhor interesse do utilizador, na busca pela efetividade da proteção e da autodeterminação informativa no caso concreto.

4 CONCLUSÃO

O alvorecer do Século XXI vem marcado pela ascensão do fenômeno do capitalismo de vigilância, termo cunhado por Shoshana Zuboff. A nova conformação vem marcada pela ascensão vertiginosa das empresas de tecnologia e as tecnologias de informação e comunicação por elas desenvolvidas. E, impulsionada pela lógica do mercado, agora avidamente interessado pelas “pontocom”, a relação entre o usuário e controlador, naturalmente assimétrica, fica marcada por violações as mais variadas. Seja pela publicidade direcionada, seja pelo esforço em alterar o comportamento do utilizador, o capitalismo de vigilância é fenômeno atual, inédito, e considerado nocivo, devendo ser regulado, e, em certa medida, combatido.

Ao longo deste trabalho, foi possível compreender o surgimento do fenômeno

descrito por Zuboff, desde as decisões cruciais do Google em 2002 e sua relação com instituições estadunidenses, até as nocividades da dinâmica capitalista vivenciadas desde então. Foram trazidos casos emblemáticos, como o escândalo da aplicação *Street View* e o caso da atuação da Cambridge Analytica nas eleições dos Estados Unidos em favor do então candidato Donald Trump. Foram trazidos, ainda, os casos referentes à técnica de *geoblocking* e *geopricing* praticadas pela empresa Decolar.com, a divulgação da gravidez da adolescente cliente da rede de lojas Target, e a coleta de dados biométricos pela concessionária da linha amarela do metrô de São Paulo.

Na sequência, considerado o estado da arte e mencionadas as diretrizes trazidas por Zuboff sobre como deve ser construída uma legislação específica de proteção de dados pessoais, houve o enfrentamento do ordenamento jurídico brasileiro tal qual se encontra no primeiro semestre de 2023. Deixou-se de enfrentar diretamente o Código de Defesa do Consumidor (Lei n. 8.078/1990), a Lei de Acesso à Informação (Lei n. 12.527/2011), a lei que tipifica os delitos informáticos (Lei n. 12.737/2012) e a Lei do Governo Digital (Lei n. 14.129/2021), porquanto tais legislações não abordam a temática dos dados pessoais no contexto de sociedade da informação. Foram compreendidos o Marco Civil da Internet, a Lei Geral de Proteção de Dados. Ambas as legislações tratam da temática da proteção de dados, porém não foi possível verificar efetividade.

Enfrentou-se, também, o julgamento das ADIs 6387, 6388, 6388, 6389, 6390 e 6393, e a Emenda Constitucional n. 115/2022, e sobreveio a conclusão de que não existe a proteção nos termos da teorização de Zuboff. Com efeito, não se verificou no ordenamento jurídico o reconhecimento do fenômeno do capitalismo de vigilância, passo importante para sua regulação.

Mesmo assim, o simples fato de haver legislações e entendimentos jurisprudenciais no sentido de reconhecer a importância da proteção dos dados pessoais e seu caráter de direito fundamental elevam o Brasil a um patamar avançado de proteção, acompanhando o ordenamento de outros países. Assim, apesar de a proteção efetiva ainda se encontrar vulnerabilizada, vislumbra-se que o ordenamento se encontra no caminho da efetivação.

A atual previsão expressa da proteção aos dados pessoais tende a evitar permissividades por parte tanto dos controladores quanto dos aplicadores e intérpretes da norma jurídica. Ainda, a atual previsão constitucional é a medida que

mais se aproxima do reconhecimento do capitalismo de vigilância vigente. Dessa forma, quando houver a análise do caso concreto, o reconhecimento do fenômeno e proteção do titular torna-se possível, pois apenas as normas infraconstitucionais não conferem a abertura necessária, especialmente diante da possibilidade de ocorrer um caso omisso, em que se faça necessária a decisão em favor do titular.

REFERÊNCIAS

ACEVES, William. Virtual Hatred: how russia tried to start a race war in the united states. **Michigan Journal Of Race & Law**, [S.L.], n. 242, p. 177, 2019. Disponível em: https://repository.law.umich.edu/mjrl/vol24/iss2/2. Acesso em: 16 jun. 2023.

ANDRADE, Diogo de Calasans Melo; BARRETO, Roberta Hora Arcieri. A ausência da atividade fiscalizadora na lei geral de proteção de dados pessoais e sua ineficácia. **Revista Eletrônica Direito e Sociedade - Redes**, [S.L.], v. 8, n. 2, p. 61-73, 8 jun. 2020. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/5407. Acesso em: 7 nov. 2022.

ARAFAN, Adam Mehdi. **Surveillance Capitalism and Nudging in Pokémon Go: A dispositif Analysis of Behavioral modification and commodification**. 2021. 63 f. TCC (Graduação) - Curso de Media En Cultuur, Utrecht University, Utrecht, 2021. Disponível em: https://studenttheses.uu.nl/handle/20.500.12932/40240. Acesso em: 22 jun. 2023.

BARRETO JUNIOR, Irineu Francisco; GALLINARO, Fábio; SAMPAIO, Vinícius Garcia Ribeiro. MARCO CIVIL DA INTERNET E DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO. **Revista Direito, Estado e Sociedade**, [S.L.], n. 52, p. 114-133, 10 set. 2018. Disponível em: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/835. Acesso em: 7 nov. 2022.

BORGES, Sabrina Nunes. A revolução da internet e os dados pessoais. In: MORAIS, José Luis Bolzan de; LOBO, Edilene (org.). **Temas de Estado de Direito e Tecnologia**. Porto Alegre: Fi, 2021. p. 171-212. Disponível em: https://www.editorafi.org/093tecnologia. Acesso em: 22 jun. 2023.

BRASIL. Congresso. Câmara dos Deputados. **Proposta de Emenda À Constituição Nº 17/2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 16 jun. 2023.

BRASIL. Congresso. Senado. **Proposta de Emenda À Constituição Nº 17/2019.** Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, Disponível em: https://www.lexml.gov.br/urn/urn:lex:br:senado.federal:proposta.emenda.constitucional;pec:2019;17. Acesso em: 16 jun. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF, Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jun. 2023.

BRASIL. **Emenda Constitucional n. 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 7 nov. 2022.

BRASIL. **Lei Geral de Proteção de Dados de 2018**. Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 7 nov. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 19 jun. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 19 jun. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 jun. 2023.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 7 nov. 2022.

BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm. Acesso em: 19 jun. 2023.

BRASIL. Supremo Tribunal Federal. Referendo em Medida Cautelar. Relatora: Ministra Rosa Weber. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.393 Distrito Federal**. Brasília, 07 maio 2020. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5896399. Acesso em: 16 jun. 2023.

CAMURÇA, Lia Carolina Vasconcelos; MATIAS, João Luís Nogueira. DIREITO À

PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS: análise das práticas obscuras de direcionamento de publicidade consoante a lei nº 13.709 de 14 de agosto de 2018. **Revista Direitos Fundamentais & Democracia**, [S.L.], v. 26, n. 2, p. 6-23, 31 ago. 2021. Centro Universitario Autonomo do Brasil. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1590. Acesso em: 16 jun. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 9 nov. 2022.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. 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**, [S.L.], v. 12, n. 2, p. 1002-1033, abr. 2021. Disponível em: https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/?format=html&lang=pt. Acesso em: 16 jun. 2023.

FRIAS, Eliana Sanches de; NÓBREGA, Lizete Barbosa da. O "PL das fake news": uma análise de conteúdo sobre a proposta regulatória. **Revista de Estudos Universitários - Reu**, [S.L.], v. 47, n. 2, p. 363-393, 17 dez. 2021. Disponível em: https://periodicos.uniso.br/reu/article/view/4803. Acesso em: 22 jun. 2023.

GOOGLE publica manifesto criticando PL das Fake News. **Jornal do Comércio.** [S.L.]. 02 maio 2023. Disponível em: https://www.jornaldocomercio.com/politica/2023/05/1104881-google-publica-manifesto-criticando-pl-das-fake-news.html. Acesso em: 19 jun. 2023.

JALIL, Simone Medeiros; BURLAMAQUI, Aquiles Medeiros Filgueira. A importância do reconhecimento da proteção de dados pessoais como direito fundamental. **Research, Society And Development**, [S.L.], v. 11, n. 14, p. 00-00, 25 out. 2022. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/32707. Acesso em: 22 jun. 2023.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, [S.L.], v. 12, n. 02, p. 01-33, 27 ago. 2020. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 16 jun. 2023.

MARTINS, Marcelo Guerra; TATEOKI, Victor Augusto. Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica. **Revista Eletrônica Direito e Sociedade - Redes**, [S.L.], v. 7, n. 3, p. 135-148, 21 out. 2019. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/5610. Acesso em: 7 nov. 2022.

MEIRELES, Adriana Veloso. Algoritmos e autonomia: relações de poder e resistência no capitalismo de vigilância. **Opinião Pública**, [S.L.], v. 27, n. 1, p. 28-50, abr. 2021.

Disponível em: https://www.scielo.br/j/op/a/vryT7RHCQ8q8RvYXF3zKvZS/. Acesso em: 7 nov. 2022.

MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. **Pensar - Revista de Ciências Jurídicas**, [S.L.], v. 25, n. 4, 11 dez. 2020. Disponível em: https://periodicos.unifor.br/rpen/article/download/10828/pdf. Acesso em: 16 jun. 2023

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO: tendências contemporâneas de materialização. **REI - REVISTA ESTUDOS INSTITUCIONAIS**, [S. l.], v. 6, n. 2, p. 507–533, 2020. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 7 nov. 2022.

MENEZES NETO, Elias Jacob de; BOLZAN DE MORAIS, José Luis. A FRAGILIZAÇÃO DO ESTADO-NAÇÃO NA PROTEÇÃO DOS DIREITOS HUMANOS VIOLADOS PELAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO. **Revista Direitos Fundamentais & Democracia**, [S. l.], v. 23, n. 3, p. 231–257, 2018. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1135. Acesso em: 7 nov. 2022.

MORAIS, Jose Luis Bolzan de. O Estado de Direito “confrontado” pela “revolução da internet”! In: MORAIS, José Luis Bolzan de; LOBO, Edilene (org.). **Temas de Estado de Direito e Tecnologia**. Porto Alegre: Fi, 2021. p. 14-48. Disponível em: https://www.editorafi.org/093tecnologia. Acesso em: 22 jun. 2023.

MORELLATO, Ana Carolina Batista; SANTOS, André Filipe Pereira Reid dos. O Capitalismo de vigilância e a lei geral de proteção de dados: Anonimização e consentimento. **Revista Brasileira de Sociologia do Direito**, v. 8, n. 2, pp. 184-211, 4 maio 2021. Disponível em: https://doi.org/10.21910/rbsd.v8i2.455. Acesso em: 7 nov. 2022.

PL das Fake News: Telegram dispara mensagem a usuários contra projeto. **Exame.** [S.L.]. 09 maio 2023. Disponível em: https://exame.com/brasil/telegram-envia-mensagem-a-usuarios-contra-pl-das-fake-news/. Acesso em: 19 jun. 2023.

QUEIROZ, Renata Capriolli Zocatelli. **A proteção de dados pessoais: a LGPD e a disciplina jurídica do encarregado de proteção de dados pessoais**. 2021. 137 f. Tese (Doutorado) - Curso de Direito, Universidade de São Paulo, São Paulo, 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-085834/pt-br.php. Acesso em: 16 jun. 2023.

SANTOS, Josilenni de Alencar Fonseca. **A Proteção de Dados como um Direito Fundamental no Brasil**: uma análise da sua fundamentalidade material para a construção de uma estrutura dogmática. 2021. 101 f. Dissertação (Mestrado) - Curso de Direito, Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Teresina, 2021. Disponível em: https://repositorio.idp.edu.br/handle/123456789/3351. Acesso em: 16 jun. 2023.

THE GUARDIAN: Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. 00, 17 mar. 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 16 jun. 2023.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, [S.L.], v. 30, n. 86, p. 269-285, abr. 2016. Disponível em: https://www.scielo.br/j/ea/a/n87YsBGnphdHHBSMpCK7zSN/abstract/?lang=pt. Acesso em: 16 jun. 2023.

WEIL, Nancy. '98 was 'terrific' year for PCs, Dataquest says. **Cable News Network.** Boston. 1 fev. 1999. Disponível em: http://edition.cnn.com/TECH/computing/9902/01/terrific.idg/index.html. Acesso em: 13 maio 2023.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2020. p.i.