

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

Cássio Sbicigo Martins

**A FUNÇÃO SOCIAL DAS *BIG TECHS*:**  
PERSPECTIVAS DO TITULAR DE DADOS BRASILEIRO EM UM  
CONTEXTO DE CAPITALISMO DE VIGILÂNCIA E EUROPEIZAÇÃO  
NORMATIVA

Santa Maria, RS  
2023

Cássio Sbicigo Martins

**A FUNÇÃO SOCIAL DAS *BIG TECHS*:**  
PERSPECTIVAS DO TITULAR DE DADOS BRASILEIRO EM UM CONTEXTO DE  
CAPITALISMO DE VIGILÂNCIA E EUROPEIZAÇÃO NORMATIVA

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

Orientador: Prof. Me. João Pedro Seefeldt Pessoa

Santa Maria, RS, Brasil  
2023

**Cássio Sbicigo Martins**

**A FUNÇÃO SOCIAL DAS *BIG TECHS*:  
PERSPECTIVAS DO TITULAR DE DADOS BRASILEIRO EM UM CONTEXTO DE  
CAPITALISMO DE VIGILÂNCIA E EUROPEIZAÇÃO NORMATIVA**

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

Aprovado em 29 de novembro de 2023.

---

João Pedro Seefeldt Pessoa, Me. (UFSM)  
(Presidente/Orientador)

---

Angela Araujo da Silveira Espindola, Dra. (UFSM)  
(Avaliadora)

---

Rafael Santos de Oliveira, Dr. (UFSM)  
(Avaliador)

Santa Maria, RS  
2023

## **DEDICATÓRIA**

*À minha pequena família nuclear, o anjo que chamo de mãe e meu pai de coração  
Aos amigos que tiram o peso dos dias  
E aos que acreditaram em mim mais do que eu mesmo jamais pude acreditar*

## **AGRADECIMENTOS**

Agradeço ao meu orientador Prof. João Pedro Seefeldt Pessoa, pela sabedoria e disponibilidade sem as quais este trabalho não seria possível. Agradeço à profa. Angela Araujo da Silveira Espindola pela presença essencial ao longo da graduação e por despertar meu interesse pela pesquisa.

*Deixem dormir o futuro como merece.  
Se o acordam antes do tempo,  
teremos um presente sonolento (KAFKA, 1931)*

## RESUMO

### A FUNÇÃO SOCIAL DAS *BIG TECHS*: PERSPECTIVAS DO TITULAR DE DADOS BRASILEIRO EM UM CONTEXTO DE CAPITALISMO DE VIGILÂNCIA E EUROPEIZAÇÃO NORMATIVA

AUTOR: Cássio Sbicigo Martins  
ORIENTADOR: João Pedro Seefeldt Pessoa

A presente pesquisa busca explorar as perspectivas do titular de dados frente à lógica contemporânea de exploração de dados, instituída pelas *big techs*, e o fenômeno de difusão internacional de leis de regulação de dados a partir da União Europeia. Pergunta-se se é possível pensar a função social da empresa, aplicada à *big techs*, como ferramenta para uma legislação de dados emancipatória, que melhor corresponda à realidade brasileira, com base no ordenamento jurídico nacional. Para tanto, emprega-se o método de abordagem fenomenológico e a pesquisa bibliográfica para compor uma compreensão holística dos diversos fenômenos sociológicos, econômicos e jurídicos analisados. Os métodos de procedimento empregados na realização da pesquisa são o comparativo e o monográfico. Inicialmente, empreende-se um estudo cronológico das evoluções tecnológicas que resultam no atual estado da arte da exploração de dados, contrastando compreensões mais esperanças da economia digital surgidas à época do advento da *internet* com teóricos contemporâneos, críticos do regime de exploração instituído pelas *big techs* e da despolitização do debate tecnológico. Define-se o capitalismo de vigilância e a evolução das regulações sobre privacidade e proteção de dados ao longo dos anos. Em um segundo momento, explora-se o fenômeno da difusão internacional de normas através da teoria do Efeito Bruxelas, constatando-se o poder da União Europeia exercer influência *de facto* e *de jure* em outras jurisdições. Na sequência, verifica-se a ocorrência do Efeito Bruxelas no Brasil, comparando-se as duas principais leis de proteção de dados tratadas neste trabalho, o Regulamento Geral de Proteção de Dados Europeu (RGPD) e a Lei Geral de Proteção de Dados Pessoais (LGPD). Tendo em vista o papel subalterno do Brasil tanto no aspecto tecnológico quanto legislativo, e considerando que a realidade do titular de dados nacional é moldada por interesses estrangeiros, reconhece-se um contexto geral de colonialismo de dados, sendo a lei nacional um reflexo de motivações mercadológicas externas e, por isso, insuficiente para responder à realidade brasileira. A partir de um pensamento decolonial e pós-abissal, busca-se construir uma alternativa autóctone de proteção jurídica a partir de uma leitura integrada do ordenamento. A aplicação do princípio da função social da empresa às *big techs* perpassa a interpretação de diversos diplomas para efetivar os direitos do titular de dados, de forma a trazer a discussão da proteção de dados à esfera coletiva e melhor responder às necessidades da população brasileira.

**Palavras-chave:** *Big techs*; LGPD; Função social; Colonialismo.

## ABSTRACT

### **THE SOCIAL FUNCTION OF *BIG TECHS*: PERSPECTIVES OF THE BRAZILIAN DATA SUBJECT IN A CONTEXT OF SURVEILLANCE CAPITALISM AND NORMATIVE EUROPEANIZATION**

AUTHOR: Cássio Sbicigo Martins  
ADVISOR: João Pedro Seefeldt Pessoa

The present research aims to explore the perspectives of data subjects in the face of the contemporary logic of data exploitation established by big tech companies and the international diffusion phenomenon of data regulation laws originating from the European Union. The question is whether it is possible to consider the social function of the company, applied to big tech companies, as a tool for emancipatory data legislation that better corresponds to the Brazilian reality, based on the national legal system. To do so, the phenomenological approach method and bibliographic research are employed to form a holistic understanding of various sociological, economic, and legal phenomena analyzed. The procedural methods used in the research are comparative and monographic. Initially, a chronological study is undertaken on technological developments leading to the current state of data exploitation, contrasting more hopeful understandings of the digital economy that emerged at the time of the internet's advent with contemporary theorists critical of the exploitation regime instituted by big tech companies and the depoliticization of the technological debate. The concept of surveillance capitalism and the evolution of regulations on privacy and data protection over the years are defined. In a second phase, the phenomenon of the international diffusion of norms through the theory of the Brussels Effect is explored, noting the power of the European Union to exert influence *de facto* and *de jure* in other jurisdictions. Subsequently, the occurrence of the Brussels Effect in Brazil is examined, comparing the two main data protection laws addressed in this work: the General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD). Given Brazil's subordinate role in both technological and legislative aspects, and considering that the reality of the national data subject is shaped by foreign interests, a general context of data colonialism is recognized, with national law reflecting external market motivations and therefore being insufficient to address the Brazilian reality. From a decolonial and post-abysal perspective, the aim is to build an autochthonous alternative for legal protection based on an integrated reading of the legal system. The application of the principle of the social function of the company to big tech companies involves the interpretation of various legal instruments to enforce data subject rights, bringing the discussion of data protection to the collective sphere and better addressing the needs of the Brazilian population.

**Keywords:** *Big techs*; LGPD; Social function; Colonialism.



## SUMÁRIO

<b>1. INTRODUÇÃO.....</b>	<b>9</b>
<b>2. A PROTEÇÃO DE DADOS NO CAPITALISMO DE VIGILÂNCIA E SUA REGULAÇÃO .....</b>	<b>12</b>
2.1. <i>INTERNET, BIG TECHS</i> E O CAPITALISMO DE VIGILÂNCIA .....	12
2.2. A REGULAÇÃO DA PROTEÇÃO DE DADOS .....	18
<b>3. LEI GERAL DE PROTEÇÃO DE DADOS E A EUROPEIZAÇÃO NORMATIVA .....</b>	<b>25</b>
3.1. EUROPEIZAÇÃO NORMATIVA E O RGPD .....	25
3.2. A LGPD E O RGPD .....	29
<b>4. A FUNÇÃO SOCIAL DAS <i>BIG TECHS</i> .....</b>	<b>36</b>
4.1. INADEQUAÇÕES DA LGPD À REALIDADE BRASILEIRA: COLONIALISMO DE DADOS E MOTIVAÇÕES MERCADOLÓGICAS.....	36
4.2. FUNÇÃO SOCIAL DAS <i>BIG TECHS</i> : POSSIBILIDADES DE UMA LEGISLAÇÃO DE DADOS EMANCIPATÓRIA .....	43
<b>5. CONCLUSÃO.....</b>	<b>53</b>
<b>REFERÊNCIAS .....</b>	<b>56</b>

## 1. INTRODUÇÃO

No atual contexto de um mundo globalizado, a tecnologia da informação e comunicação é indissociável da vida em sociedade. Serviços essenciais para os negócios, educação e organização pessoal dos indivíduos são prestados por grandes empresas multinacionais de tecnologia. O titular de dados adquire papel central nessa lógica, já que a rentabilidade do modelo de publicidade adotado por essas plataformas depende dos seus dados para negociação com os anunciantes. Dessa forma, o usuário cede seus dados em troca da promessa de melhorias dos serviços prestados. O reconhecimento dessa nova forma de capitalismo ensejou a criação de leis de proteção de dados ao redor do mundo, para resguardar os usuários das plataformas da exploração predatória de seus dados.

É notório que o direito frequentemente demora para responder às mudanças sociais, e tal fato é especialmente verdade no que diz respeito à tecnologia. Pela própria natureza do processo legislativo, ele se encontra em descompasso perpétuo com o imediatismo que caracteriza a inovação em áreas como a tecnologia informacional e inteligência artificial nos últimos anos. Parcela significativa dessas inovações é produto de um seleto grupo de empresas originárias da região Vale do Silício, nos Estados Unidos, chamadas *big techs*, as maiores empresas de tecnologia do mundo. Difundidas internacionalmente, as ações de empresas como a Google, Facebook e Apple impactam diretamente a economia em escala global.

A discussão sobre a proteção de dados culmina com o Regulamento Geral de Proteção de Dados (RGPD), regulamento europeu em vigência desde 2018, que representa um dos mais importantes marcos legislativos internacionais, influenciando fortemente a atividade legiferante em diversos países em desenvolvimento, incluindo o Brasil, na forma de sua própria Lei Geral de Proteção de Dados Pessoais (LGPD). Em que pese seja importante para o país atualizar-se na temática de proteção de dados frente à comunidade internacional, a mera transposição de uma norma diversa ao ordenamento nacional pode trazer consigo discursos, práticas e interesses que refletem melhor a realidade dos países que a difundiram do que a realidade brasileira.

Haja vista a clara existência de uma motivação mercadológica para a adoção de um modelo estrangeiro de legislação, justifica-se uma análise mais minuciosa desse processo, e o quanto ele prioriza a instauração de um sistema de mercantilização de dados antes dos direitos do titular. Ademais, é razoável imaginar que um titular de dados oriundo de um país com altos índices de analfabetismo, desemprego e pobreza, que não exporta tecnologia e tampouco consolidou seu Estado social, possua uma relação diferente com a tecnologia, se comparado com titulares em países desenvolvidos. Em outras palavras, é possível que haja mais

hipossuficiência na relação de consumo, mais assimetria informacional e menos alternativas de resposta. Essa realidade é sintomática de uma nova forma de colonialidade que encontra campo fértil na ideologia neoliberal, na qual os países do Norte global detêm o monopólio da tecnologia de exploração dos países do Sul.

A pesquisa se justifica ao propor uma discussão sobre *big techs* considerando a realidade social brasileira, desvinculada de uma postura incauta frente aos avanços tecnológicos e à lógica de acumulação capitalista. Não se despreza os avanços trazidos pela LGPD, mas argumenta-se que esses avanços não bastam para a realidade de vulnerabilidade do titular de dados brasileiros, na medida em que o modelo adotado de lei de proteção de dados também opera para legitimar a lógica de exploração empreendida pelas *big techs*.

Portanto, o presente trabalho busca explorar as perspectivas de direito do titular de dados brasileiro e a função social das *big techs*, frente à lógica mercantilista do capitalismo de vigilância e das regulamentações eurocêntricas de proteção de dados. Trata-se do Brasil, na condição de país emergente frente à comunidade internacional, a partir do advento das *big techs* como instituidoras do modelo de exploração de dados vigente, ou seja, com o recorte temporal aproximado das últimas duas décadas. Nesse contexto, seria possível pensar a função social das *big techs* como ferramenta para uma legislação de dados emancipatória, que melhor corresponda à realidade brasileira, com base no ordenamento jurídico nacional?

Esta pesquisa se utilizará da bibliografia mais recente sobre o tema, análise legal e embasamento jurídico para compor um panorama dos diversos fenômenos sociológicos, econômicos e jurídicos que formam o atual estado de coisas. Para tanto, será utilizado o método fenomenológico, considerando que se trata de temática complexa, dinâmica e incipiente, a respeito da qual as principais teorias ainda estão se consolidando. O método se adequa à pesquisa, na medida em que observa os fenômenos conforme eles aparecem à consciência, a partir de detalhada análise do mundo. Dessa forma, o pesquisador reconhece-se como parte dos fenômenos que observa, e a consciência é um esforço ativo, empregado livre de suposições e estruturas prévias.

Os métodos de procedimento empregados na realização da pesquisa serão o comparativo e o monográfico. O método comparativo será utilizado para identificar as correspondências entre as legislações de proteção de dados europeia (Regulamento Geral sobre a Proteção de Dados – RGPD) e brasileira (Lei Geral de Proteção de Dados – LGPD), no que tange às normas e princípios. O método monográfico será empregado para a observação dos efeitos do capitalismo de vigilância, análise da adequação da Lei Geral de Proteção de Dados à realidade brasileira e propositura de um uso social da tecnologia da informação. Será empregada a técnica

de pesquisa bibliográfica, na forma das principais obras e pesquisas acadêmicas contemporâneas sobre a temática.

A presente pesquisa está dividida em três partes. Inicialmente, faz-se necessário um breve histórico do contexto tecnológico que deu origem às *big techs*, e como a lógica mercantil de dados sob a qual essas empresas operam deu origem ao chamado capitalismo de vigilância ou capitalismo de plataforma, conceituando o regime de exploração de dados do usuário titular. Da mesma forma, busca-se compreender o desenvolvimento do direito à proteção de dados e suas regulações desde sua origem e conceituação, na forma do direito à privacidade, até as legislações contemporâneas, e sua inclusão no rol de direitos fundamentais.

Em um segundo momento, explora-se o fenômeno de europeização normativa no contexto internacional, demonstrando como a União Europeia é capaz de regular unilateralmente determinados mercados mundiais e influenciar na adoção de determinados modelos legislativos. Na sequência, busca-se verificar em que medida o fenômeno de difusão internacional das regulamentações de proteção de dados pessoais a partir do Regulamento Geral de Proteção de Dados RGPD europeu se manifesta no Brasil, na forma da Lei Geral de Proteção de Dados Pessoais (LGPD).

Por fim, busca-se responder o problema de pesquisa mediante exploração das perspectivas do titular de dados brasileiro, considerando os descompassos da legislação com a realidade nacional e o contexto de colonialismo de dados. Assim, pondera-se a necessidade de um arcabouço jurídico propriamente brasileiro com o auxílio do pensamento decolonial, inserindo a proteção de dados em uma dimensão de direitos coletivos e difusos e buscando-se uma alternativa jurídica emancipatória a partir da função social da empresa.

## 2. A PROTEÇÃO DE DADOS NO CAPITALISMO DE VIGILÂNCIA E SUA REGULAÇÃO

O tratamento de dados é um dos temas mais pertinentes da contemporaneidade, gerando consequências interpessoais, sociológicas e jurídicas. O atual contexto tecnológico estabeleceu os dados como um novo recurso essencial, indispensável para a lógica de mercado instituída principalmente pelas grandes empresas de tecnologia. A história da proteção de dados se desenvolve em paralelo a essa realidade, com regulações nacionais e internacionais buscando dar adequada proteção aos direitos fundamentais em risco frente à vigilância empreendida através das novas tecnologias.

Dessa forma, o aprofundamento da discussão demanda uma compreensão holística das tecnologias que tornaram possível essa dinâmica e quais as implicações de sua ubiquidade nos dias atuais, bem como uma análise da evolução do direito à privacidade, que embasou o desenvolvimento dessas regulações ao longo do tempo até o estado da arte atual.

### 2.1. *INTERNET, BIG TECHS* E O CAPITALISMO DE VIGILÂNCIA

O advento da *Internet* revolucionou a relação do indivíduo com a informação, na medida em que ações e objetos passam a ser representados digitalmente, ou “informatizados”, gerando dados. Autores que escrevem sobre a popularização da *Internet* na virada do século XXI o fazem com entusiasmo, ingenuidade e otimismo. As origens da rede remontam à Guerra Fria, e à demanda do governo estadunidense para desenvolver linhas de comunicação capazes de sobreviver a um ataque nuclear. Desse projeto, surge a *Arpanet*, no Departamento de Defesa dos Estados Unidos, utilizando-se da tecnologia então conhecida como comutação de pacotes (ABREU, 2009, p. 2).

A década de 1970 testemunhou os primeiros “nós” na rede, estabelecidos nas universidades da Califórnia e de Utah, bem como notáveis avanços empreendidos por professores de Harvard e do Massachusetts *Institute of Technology* (CASTELLS, 2001, p. 9). Um destaque importante é a criação do protocolo intra rede (IP), padrão sob o qual a rede opera até hoje. Nesse contexto, a *Arpanet* se afasta dos usos militares e passa a ser utilizada para fins acadêmicos e informacionais. Em 1989, Tim Berners-Lee implementou o software que permitia obter informação de qualquer computador conectado através da *Internet*, por meio de um sistema de distribuição de hipertexto (HTTP), que premeditava a abertura da rede para o público em geral nos anos 90, vista como a máxima expressão da experiência democrática (TURNER,

MUÑOZ, 2002, p. 35).

Embora os avanços mais importantes para a origem da *Internet* tenham ocorrido em instituições governamentais e importantes centros de pesquisa, foi o interesse comercial que consolidou, de forma definitiva, a tecnologia na vida moderna. Nos anos 90, empresários do Vale do Silício financiaram o primeiro navegador comercial, o *Netscape Navigator*; simultaneamente, a Microsoft desenvolvia seu sistema operacional (*Windows 95*), e seu próprio navegador, o *Internet Explorer* (CASTELLS, 2001, p. 19). Assim, a internet se privatizava e abria-se às possibilidades de mercado, que viriam a moldar o ambiente virtual e o comportamento do consumidor.

Em 2001, Castells assim definia a nova economia:

Apliquemos agora esses mecanismos (da economia eletrônica) a um processo de inovação que ocorre num sistema de fonte aberta e é facilitado por interação on-line. Um produto de qualidade superior (por exemplo, um programa de software) é gerado pelo esforço coletivo de uma rede, um esforço em que cada participante encontra uma compensação no esforço livremente empenhado por outros. Assim, a inovação continua sendo o produto de trabalho inteligente, mas de um intelecto coletivo. Nenhum departamento de pesquisa é capaz de rivalizar com o poder de uma rede global, cooperativa - na verdade, é assim que a ciência básica se desenvolve, com retornos extraordinários (...) A lógica da cooperação e da fonte aberta como prova de fogo da inovação não se limita ao software. Ela é a lógica que permeia toda a indústria de serviços online, uma vez que os portais dão acesso à informação e serviços, como uma maneira de vender publicidade e obter informação que possa ser reutilizada para fins de marketing. Nessa lógica, os compradores são produtores, já que podem fornecer informação crítica por seu comportamento, e por suas demandas, ajudando constantemente as companhias eletrônicas a modificar seus produtos e serviços. Na prática empresarial orientada para compradores, a capacidade de interagir com compradores como fontes de informação crítica torna-se um componente essencial do modelo empresarial (CASTELLS, 2001, p. 85-86).

Mais de duas décadas depois, percebe-se que Castells e seus contemporâneos descreveram acuradamente as características da economia pós-revolução informacional, mas não previram os moldes nos quais estas se manifestaram. A contracultura tecnocrata estadunidense adotou uma ideologia neoliberal, encabeçada por figuras como Steve Jobs, que sobrepôs outras culturas *hacker* emancipatórias existentes na Europa e em outros lugares do mundo. Trata-se de desenvolver uma narrativa anti-institucional e emancipatória, ignorando-se o fato de que toda essa tecnologia foi financiada pelo governo estadunidense, e a suposta emancipação deve ser buscada no mercado (MOROZOV, 2018, p. 16).

As empresas responsáveis por instituir essa lógica são as *big techs*, empresas de tecnologia de sucesso, a maioria das quais originárias da região da Califórnia conhecida como Vale do Silício. O protagonismo das *big techs* desde a década de 1990 no mercado da tecnologia informacional é espelhado pela imprescindibilidade dos serviços oferecidos por elas para

usuários ao redor do mundo. Em razão disso, os nomes de algumas *big techs* são quase sinônimos de seus serviços, sejam eles resultantes de avanços tecnológicos capitaneados por elas ou não. Quanto à nomenclatura, importa referir que várias destas empresas hoje estão formando *holdings* e se transformando em conglomerados (*Alphabet, Meta*). Doravante, serão referidas pelo nome do serviço pelo qual são reconhecidas, e não pelo nome empresarial.

A ascensão das *big techs* tem, na sua origem, a mesma fórmula universalmente associada com a inovação tecnológica: a parceria entre empresários vendendo soluções tecnológicas e capitalistas de risco. Com o aporte financeiro dos “investidores anjos”, pequenas empresas de tecnologia no Vale do Silício transformaram suas ideias em negócios. A estratégia é mudar o mundo através da tecnologia, e depois ser recompensado com dinheiro e poder, por meio das operações do mercado financeiro (CASTELLS, 2001, p. 49-53). Ao longo da década de 1990, histórias de sucesso como as da Sun Microsystems e Yahoo propulsionaram a narrativa de engenheiros idealistas se tornando chefes de empresas gigantescas (que ainda operam como *startups*), isentos de qualquer tipo de responsabilidade social, desde que atuem em nome do progresso da tecnologia (FOROOHAR, 2019, p. 41-57).

A *big tech* mais bem sucedida é a Google, e sua trajetória é paradigmática para adoção do modelo atual de coleta de dados. Larry Page e Sergey Brin, fundadores da empresa, se conheceram durante o doutorado em engenharia da computação na Universidade de Stanford, na Califórnia. Seguindo os passos de Tim Berners-Lee anos antes, os empresários entendiam o ciberespaço como um grande número de itens identificados e conectados entre si por *hyperlinks*, porém desorganizados, o que traria grandes benefícios para quem organizasse primeiro. Assim, desenvolveram o *software* chamado *BackRub*, que era capaz de categorizar os resultados mais relevantes na rede, baseando-se no número de citações que cada endereço tinha em outros *hyperlinks* (FOROOHAR, 2019, p. 53).

À época de sua criação, a Google atendeu uma grande demanda pela navegabilidade e uso eficiente da *World Wide Web*. Inicialmente adotando o mantra “não seja mau” (*don't be evil*), a empresa revolucionou o ambiente online com sua proposta de acessibilidade e organização (VAIDHYANATHAN, 2011, p. 30-40). Contudo, o *modus operandi* da empresa, desde a sua concepção, envolvia uma violação de *copyrights* generalizada, que passou largamente ignorada pelas autoridades em face das inovações trazidas. Page e Brin justificaram que tais avanços seriam impossibilitados se todos os afetados pelas mudanças tivessem que ser previamente consultados. A mesma justificativa é apresentada que tange à responsabilidade pelo conteúdo disseminado na rede, senão vejamos:

A mensagem era que o debate se daria em termos tecnológicos, ou não aconteceria. (...) Talvez seja por isso que, desde o início, as regras favoreceram a indústria sobre os consumidores que eles supostamente servem. O mais notório exemplo de regra “especial” que beneficia a Big Tech é o cartão de livre conduta trazido pela seção 230 do Communications and Decency Act of 1996 (CDA), que escusa empresas de tecnologia de responsabilidade por quase qualquer tipo de conteúdo ilegal ou ação perpetrada por seus usuários (existem algumas pequenas exceções nos casos de violações de copyright e certos crimes federais). (...) A ideia era que meros empresários implementando quadros de mensagens online, grupos de conversa ou navegadores incipientes de seus porões e garagens simplesmente não tinham os recursos ou mão de obra para monitorar as ações dos usuários, e que requerer que eles o fizessem impediria o desenvolvimento da Internet. Os tempos, é claro, mudaram. Hoje, Facebook, Google e outras companhias absolutamente *podem* - e de fato fazem - monitorar quase tudo que fazemos online. Ainda assim, querem ficar dos dois da cerca no que diz respeito a se responsabilizar pelo discurso de ódio, anúncios políticos financiados por russos e notícias falsas que se proliferam em suas plataformas. Aparentemente, eles não têm nenhuma dificuldade em rastrear toda compra que fazemos, todo anúncio em que clicamos e todas as notícias que lemos, mas limpar artigos de sites conspiratórios duvidosos, bloquear comentários anti semitas ou identificar *bots* russos ainda se prova uma tarefa muito onerosa. É porque fazer isso requer seres humanos reais ganhando rendas reais e usando julgamento real - e isso é algo que companhias de plataforma que cresceram nas costas da automatização têm tentado evitar (FOROOHAR, 2019, p. 55-56).

Os dirigentes da Google eventualmente adotaram o chamado modelo de publicidade, que envolve a aquisição de dados de usuários para a produção de algoritmos capazes de ofertar publicidade por meio de um modelo de leilão exclusivo (ZUBOFF, 2018, p. 17-68). A rentabilidade sem precedentes desse modelo impulsionou outras empresas de tecnologia a seguirem o mesmo caminho, expandindo tanto a capitalização das *big tech* quanto a abrangência da coleta de dados.

Além da Google, outras *big techs* de relevo merecem menção: a Microsoft, dominadora original do mercado de sistemas operacionais; a Apple, conhecida inicialmente por suas inovações em *hardware*; a Amazon, fundada no *e-commerce*; e a Facebook, revolucionária no âmbito das redes sociais. Todas essas empresas expandiram seus modelos de negócio de modo a gerar impactos relevantes na vida de consumidores ao redor do mundo. Uma avaliação do faturamento dessas empresas, medida por hora, no primeiro semestre de 2023, revelou uma média de US\$59 milhões para a Amazon, US\$43,9 milhões para a Apple, US\$24,5 milhões para a Microsoft e US\$13,3 milhões para Facebook. A maioria delas possui valor de mercado estimado acima de 1 trilhão de dólares.<sup>1</sup>

Particularmente relevante para este trabalho é que todas essas empresas são dos Estados

---

<sup>1</sup>BORNELI, Junior. Apple, Google e mais: quantos milhões as big techs ganham por hora. **Startse**, 2023. Disponível em: <https://www.startse.com/artigos/volume-de-receita-por-hora-das-big-techs/>



Unidos da América. Não é por acaso que a circulação de novas tecnologias se dá do Norte para o Sul global, enquanto o fluxo transfronteiriço de dados faz o caminho inverso (SILVEIRA, 2021, p. 48). Os Estados Unidos ocuparam uma posição privilegiada durante o século XX para “mudar o mundo” através da tecnologia, saindo favorecidos no período pós-guerra para investirem valores inimagináveis em sua corrida tecnológica, sob o pretexto de segurança de Estado, prescindindo de um Estado Social de Bem Estar e, posteriormente, contando com um índice de concentração de renda suficientemente alto para que alguns poucos milionários pudessem dar asas aos sonhos impossíveis de jovens empreendedores.

Não se ignora o fato de que empresas chinesas e russas de tecnologia estejam ganhando espaço no mercado. Todavia, as aspirações dessas empresas não parecem ser de quebrar a lógica estabelecida pelo Estados Unidos, mas participar ativamente do mesmo jogo (MOROZOV, 2018, p. 13-26). Quanto aos demais países emergentes que não exportam tecnologia, tanto mais estão sujeitos aos caprichos das *big techs*, na medida em que se normaliza que o faturamento das cinco empresas citadas, em 2019, tenha sido metade do PIB do Brasil (SILVEIRA, 2021, p. 44). O imenso impacto desse novo capitalismo não é o mesmo em todos os lugares do mundo.

Para Morozov, foi dessa forma que o financiamento coletivo (*crowdfunding*), louvado por Castells, foi substituído por uma espécie de solucionismo neoliberal, no qual serviços que deveriam ser prestados pelo Estado são assumidos por plataformas e empresas bilionárias. Assim, “a aldeia global jamais se materializou - em vez disso, acabamos em um domínio feudal, nitidamente partilhado entre as empresas de tecnologia e os serviços de inteligência” (MOROZOV, 2018, p. 15). De fato, a interação com o consumidor, na condição de titular de dados, é praxe para toda e qualquer empresa de tecnologia. Todavia, o modelo foi assimilado a uma lógica de acumulação capitalista desregulada, que garantiu à determinadas empresas o monopólio da inovação, e a adesão irrestrita do usuário, em todas as esferas de sua vida.

De acordo com Shoshana Zuboff, ao longo da história da humanidade, o capitalismo sempre rumou em direção a uma lógica de acumulação própria de cada época, do capitalismo industrial ao capitalismo financeiro. Com a introdução da computação e, posteriormente, da *Internet* e das relações mediadas digitalmente, objetos e ações passaram a ser “informatizados”, ou seja, representados simbolicamente, gerando dados. A atual manifestação do capitalismo, o capitalismo de vigilância, é o resultado do encontro da lógica de acumulação com a mediação por computadores (ZUBOFF, 2018, p. 17-68). Dessa forma, o processo de digitalização é mais do que o reflexo das relações a partir de novas infra estruturas que processam dados, mas uma mudança do paradigma econômico e comportamental que afeta diretamente as condições de vida a partir da ubiquidade do tratamento de dados (SARLET, 2021, p. 26). Nesse sentido:

O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como *superávit comportamental* do proprietário, alimentando avançados processos de fabricação conhecidos como “inteligência de máquina” e manufaturado em *produtos de predição* que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de *mercados de comportamentos futuros*. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro (ZUBOFF, 2021, p. 22-23).

O que Zuboff designou *superávit comportamental* constitui o motor do modelo de publicidade adotado pela Google e depois apropriado por outras *big techs*. Trata-se do excesso de dados produzidos que não é aplicado no aprimoramento do serviço, tampouco descartado, mas reorientado para “melhorar a lucratividade de anúncios tanto para o Google quanto para seus anunciantes”, por meio de sistemas de aprendizado de máquina (ZUBOFF, 2021, p. 97). Portanto, os dados adquirem valor de mercado na medida em que alimentam o aprendizado de máquina. Por sua vez, a máquina opera prevendo resultados e minimizando chances de erro, em resposta à volatilidade e especulação do mercado. Essa lógica complexa resulta em uma “vida assistida”, regulada por algoritmos (MOROZOV, 2018, p. 83).

O início do século XXI foi marcado por um otimismo acrítico frente ao crescimento desenfreado das *big techs* e aos avanços tecnológicos. Todavia, os últimos anos suscitaram preocupações diante do poder dessas empresas, suas práticas e onipresença na vida dos usuários. O capitalismo de vigilância e as ações das *big techs* trazem problemas de ordem psicológica, econômica e institucional. O regime de dominação algorítmica prescinde de meios convencionais de controle dos corpos, pois opera em paralelo com a vida cotidiana. Enquanto usuário de serviços indispensáveis para a vida moderna em sociedade, o sujeito no capitalismo de vigilância supõe-se livre e autêntico, ignorante da lógica de produção e controle na qual está imerso (HAN, 2022, p. 9).

Mas a manipulação indevida da *big data* provou ser capaz de gerar consequências muito além da esfera individual da privacidade, particularmente no que diz respeito à política. Assim ilustra Giuliano Da Empoli:

Para além dos casos particulares, que foram objeto de numerosas investigações jornalísticas ou judiciais, é possível tirar pelo menos duas conclusões de caráter mais geral. Em primeiro lugar: uma máquina superpoderosa, concebida originalmente para

mirar com precisão incrível em cada consumidor, seus gostos e suas aspirações, irrompeu na política. (...) O Facebook e as outras redes sociais são plataformas publicitárias que põem à disposição das empresas instrumentos extraordinariamente avançados para chegar a seus clientes. Mas, uma vez criada, fica claro que essa máquina pode igualmente ser utilizada para fins políticos, como realmente ocorreu nos últimos anos (...) Em segundo lugar: graças a essa máquina, as campanhas eleitorais cada vez mais se tornam verdadeiras guerras entre softwares, durante as quais os oponentes se enfrentam com a ajuda de armas convencionais (mensagens públicas e informações verdadeiras) e armas não convencionais (manipulação e fake news) com a meta de obter dois resultados: multiplicar e mobilizar seus apoios e desmobilizar as bases do adversário (EMPOLI, 2019, p. 90).

Dessa forma, a nova economia prevista por Castells se consolidou de forma muito diversa, constituindo uma realidade inescapável e perniciosa de coleta de dados sob o pretexto de melhores produtos e serviços, prestados pelas mesmas grandes empresas. A cultura neoliberal incrustada nesses avanços tecnológicos corrói instituições comuns e obstrui um debate democrático sobre o assunto, sem ceder à retórica tecnocrata. Não obstante, diversos teóricos, como os que fundamentam este texto, têm buscado reintroduzir a dimensão política no debate tecnológico. Também as instituições o fizeram, ainda que de forma díspar, a partir do momento em que a privacidade passou a representar um problema grande demais para ser ignorado. Consequentemente, a necessidade internacional de regular a esfera informacional da vida tornou-se cada vez mais premente.

## 2.2. A REGULAÇÃO DA PROTEÇÃO DE DADOS

A regulamentação da exploração de dados pessoais perpassa pela proteção do direito fundamental à privacidade, notoriamente difícil de conceituar. Os dissensos no âmbito doutrinário justificam-se pela ampla gama de interpretações do termo (vida privada, intimidade, reserva, sigilo), pela arcaica dicotomia entre público e privado, bem como pelas variadas manifestações da privacidade em diferentes países, épocas, culturas e classes sociais (FERREIRA, PINHEIRO, MARQUES, 2021, p. 155). De acordo com Doneda:

Diversos ordenamentos seguiram seus próprios caminhos ao tratar da privacidade, visto que entravam em terreno onde as particularidades de cada sociedade eram determinantes. Daí resultaram diferenças de concepção consideráveis: dentro da etiqueta da privacidade se enfileiraram estruturas voltadas para, por exemplo, garantir a ilicitude da publicação de retratos sem consentimento do retratado; o direito a abortar; a inviolabilidade do domicílio e tantas outras. Tal observação insinua que a privacidade é um termo que se presta à uma certa manipulação pelo próprio ordenamento – pois não raro ela é utilizada para suprir necessidades estruturais dele próprio, assumindo determinado sentido em função de determinadas características de um ordenamento e dificultando ainda mais a sua redução a um sentido comum

(DONEDA, 2019, p. 72-73).

A Constituição Federal de 1988, em seu art. 5º, inciso X, trata da proteção da “intimidade” e da “vida privada” (BRASIL, 1988). Para Cancelier, a privacidade é uma liberdade que, como qualquer liberdade, comporta limitações, podendo abarcar termos como “intimidade”, “vida privada” e “segredo” (CANCELIER, 2016, p. 102). A diferenciação feita pela constituinte remonta à doutrina alemã de Hubmann, na qual um esquema de esferas concêntricas cada vez mais amplas, sendo a menor a “intimidade”, a subsequente a “esfera privada” e a maior a vida pública. De acordo com Doneda, o alto grau de subjetividade envolvido na diferenciação desses conceitos por parte da doutrina justifica sua unificação na terminologia “privacidade”, contemplando a indefinição do vocábulo como uma característica ontológica própria da matéria (DONEDA, 2019, p. 74).

A discussão sobre a proteção da privacidade depende, sobretudo, de um prévio panorama histórico. A necessidade de privacidade, seja na forma do isolamento, retiro ou abstenção de contato humano, delinea-se paralelamente ao desenvolvimento da vida em sociedade. Na Grécia antiga, as atividades políticas e comuns eram relegadas ao ambiente da *pólis*, enquanto a vida particular dos indivíduos se desenvolvia no *oikos* (PESSOA, 2023, p. 28), comumente traduzido como “lar”, “casa” ou “ambiente habitado”. Contudo, não é possível associar o respeito a tais costumes de sociedades antigas com direitos individuais - na sociedade romana, a “privacidade” era mera exceção temporária às lides da *res publica* na *civitas*, onde se exercia a liberdade, não obstante muitas filosofias antigas associem o isolamento e o retiro com o desenvolvimento das virtudes ou da espiritualidade (DONEDA, 2019, p. 85).

Embora ainda não se verifique a privacidade como fenômeno social durante a Idade Média, o final deste período é marcado por uma nova arquitetura das cidades, resultado de uma concepção diferente entre indivíduo e coletividade. Em contraste à Antiguidade, a privacidade passa a ser contraposta à esfera social, e não à política. Com a economia feudal em crise e a ascensão da burguesia, a disposição das cidades reflete uma separação entre classes baseada na propriedade (DONEDA, 2019, p. 80). De acordo com Rousseau, a propriedade, que está no cerne da desigualdade entre os homens, constitui um instituto que, por ato positivo do ocupante, exclui todos os demais daquilo que é seu, gerando exclusividade de usufruto (ROUSSEAU, 2010, p. 33). Portanto, essa concepção emergente de privacidade está intimamente associada ao direito de propriedade.

Na gênese do Estado Moderno está a prerrogativa da classe burguesa por um ambiente livre de intervenções do ente público. Nesse sentido, a propriedade e sua inviolabilidade são

integrals à noção de privacidade, a ponto de configurar condição necessária para sua existência. A Revolução Industrial e a urbanização em massa intensificaram essa lógica, já que, nesse sentido:

A sociedade industrial trouxe mudanças significativas no equilíbrio entre a vida rural e urbana, já que, nas cidades, as relações entre as pessoas tendem a ser mais impessoais e a sobrevivência é marcada por um caráter mais individualista e isolacionista, perdendo algumas formas de associativismo comuns em ambientes rurais. O desenvolvimento da noção de privacidade foi impulsionado pela própria dinâmica da sociedade industrial e pela possibilidade material de garantir essa condição, especialmente com o surgimento das tecnologias de informação e comunicação (PESSOA, 2023, p. 30).

Dessa forma, as condições materiais e as novas tecnologias influenciam a noção coletiva de privacidade de forma determinante. Especialmente na Europa, a divisão do trabalho resultante do desenvolvimento do capitalismo industrial e do individualismo separou definitivamente o lar como um local destinado à vida familiar, sagrada e privada (FERREIRA, PINHEIRO, MARQUES, 2021, p. 153). Como figura jurídica autônoma, o *right to be left alone* (“direito de ser deixado só” ou “direito de ser deixado em paz”) é construção jurisprudencial atribuída a Thomas McIntyre Cooley, jurista estadunidense e Presidente da Suprema Corte de Michigan (CANCELIER, 2017, p. 217). De acordo com o jurista, o indivíduo possui um direito de imunidade completa, relacionado à personalidade, cuja função não seria apenas buscar reparação por importunações ou ofensas, mas também prevenir contra tentativas, estabelecendo limites que não podem ser ultrapassados (COOLEY, 1879, p. 29).

É nesse contexto que Samuel Warren e Louis Brandeis, em 1890, escrevem o artigo *The right to privacy*, importante marco teórico que desvincula a privacidade do direito à propriedade, agora relacionado à proteção da pessoa humana (DONEDA, 2019, p. 95).

Em seu artigo, os autores apresentam as características desse novo direito, suas funções e seus limites, distanciando-o da matriz proprietária utilizada como base para proteção de aspectos da vida privada até então, e aproximando-o da intenção de tutela da personalidade humana. Iniciam o trabalho lembrando que recentes inovações chamam a atenção para um novo nível de proteção da personalidade e para a segurança do indivíduo, chamada pelo Juiz Cooley de “direito de estar só”, visto que fotografias instantâneas e empresas de comunicação têm invadido o sagrado e privado espaço do lar, e numerosos dispositivos tecnológicos ameaçam realizar a previsão “aquilo que é sussurrado na alcova deve ser berrado do telhado”. Segundo eles, a fofoca deixou de ser um vício ocioso para tornar-se uma importante ferramenta de barganha, verdadeiro produto e comercializado como tal. Warren e Brandeis explicam que é difícil considerar o direito à privacidade como um direito proprietário em sua concepção tradicional. Tomando como exemplo os pensamentos de um pai escritos em uma carta para o seu filho ou em seu diário, revelando alguma informação íntima, defendem que ninguém que tenha acesso a tal documento poderia divulgá-lo, mesmo que o acesso tenha ocorrido de forma legítima; a proibição não seria restrita à publicação de uma

cópia da carta ou do diário em si, sendo mais ampla, atingindo o conteúdo. O que se protege não é o ato intelectual de expressar ideias em um pedaço de papel, mas os fatos que estão sendo impressos. A proteção concedida a pensamentos, sentimentos e emoções, expressados por qualquer meio é uma das instâncias de aplicação do direito a estar só, do direito a ser deixado em paz (CANCELIER, 2017, p. 218).

Dessa forma, decorrendo de razões próprias da época, é possível identificar pelo menos dois desenvolvimentos importantes relacionados à privacidade a partir do texto de Warren e Brandeis. Primeiramente, o entendimento de que a pessoa humana possui uma “personalidade inviolável”, e que garantir essa inviolabilidade é resguardar um aspecto essencial do desenvolvimento da personalidade de um indivíduo. Em segundo lugar, a associação entre a proteção da privacidade com o avanço tecnológico, já que foram justamente as novas formas de coleta e tratamento de informações emergentes à época do artigo que motivaram sua escrita (PESSOA, 2023, p. 32).

Com o surgimento da sociedade de consumo, o espaço privado da família é invadido por forças econômicas antes externas, de modo que o objetivo final do trabalho seja a aquisição de bens desejados (FERREIRA, PINHEIRO, MARQUES, 2021, p. 153). O capitalismo, antes visto como baluarte para o individualismo que dava base ao direito à privacidade, passa a ser o berço no qual novas tecnologias se desenvolvem, por sua vez capazes de transformar informações em verdadeiros ativos financeiros. Nesse contexto, a privacidade é levada ao âmbito internacional através da Declaração Universal dos Direitos Humanos de 1948, dispondo sobre a proibição de intromissões arbitrárias na vida privada (CANCELIER, 2017, p. 227).

Até então, é possível entender a privacidade como um direito negativo do Estado, com um viés individualista. As novas tecnologias, contudo, ensejam condutas ativas para coordenar o tratamento de dados, a exemplo das primeiras legislações (LUGATI; ALMEIDA, 2020, p. 4). A partir da segunda metade do século XX, o direito à proteção de dados passa essencialmente por quatro grandes momentos. O primeiro, ao final da década de 1960 e ao longo da década de 1970, buscou regular principalmente o processamento automatizado de dados pessoais frente à criação de bancos de dados (PESSOA, 2023, p. 35). Tendo em vista a nova realidade trazida pela informática, as primeiras normativas regulando o tema não se concentram tanto na proteção da privacidade individual, mas na função de processamento de dados na sociedade (RUARO, 2020, p. 233).

A Lei de Proteção de Dados do Estado de Hesse, na Alemanha, é pioneira em instituir um arcabouço de proteção de dados informatizados. O diploma contemplava apenas arquivos de titularidade pública, estipulando como tais arquivos deveriam ser armazenados e proibindo o acesso não autorizado, dispondo também sobre uma autoridade de proteção de dados.

Seguiram-se a Lei de Dados Sueca de 1973 (*Datalagen*), a lei alemã de 1977, que abrangia também dados tratados por agentes privados (*Bundesdatenschutzgesetz*), a lei austríaca de 1978, na qual destaca-se a preocupação com o fluxo transfronteiriço de dados, entre outras (LIMBERGER, 2009, p. 36).

Ao longo da segunda geração de legislações, a privacidade individual ganha ênfase, na medida que os indivíduos podiam permitir ou não o processamento de seus dados, especialmente para finalidades de *marketing* (RUARO, 2020, p. 235). Em outras palavras, o consentimento surge como figura central em algumas legislações, como condição para o processamento das informações. Dessa forma, o próprio titular é capaz de exercer seu direito fundamental. Todavia, a lógica do mero consentimento logo se mostraria insuficiente frente às mudanças tecnológicas que estavam por vir, de forma que uma nova abordagem se fazia necessária. Exemplos de legislações dessa fase são a lei francesa de 1978 (*Loi informatique et libertés*), a lei suíça de 1981 e a Lei de Dados da Noruega (LIMBERGER, 2009, p. 36).

Por sua vez, a terceira geração, desenvolvida ao longo da década de 1980, introduz o conceito de autodeterminação informativa:

Em vez da pergunta sobre se o indivíduo quer participar em processos informacionais, a questão agora muda para como o indivíduo quer participar, o que se torna mais importante (...) Novos desenvolvimentos tecnológicos e seus desafios legais afetaram a lei de proteção de dados durante a segunda e terceira geração; por causa disso, os legisladores retiraram-se da regulação ativa da tecnologia. Em vez de persistir ao longo de um difícil caminho de adaptação contínua da legislação que dá forma à tecnologia, os políticos escolheram se concentrar em mais “liberdades individuais e direitos de participação”. Consequentemente, a terceira geração enfatizou a participação e a autodeterminação. A autodeterminação na informação tem pronúncia pela primeira vez em aguda decisão do *Bundesverfassungsgericht* em 1983. Esse caso foi sobre uma tentativa alemã de realizar um censo populacional. O ato que possibilitou o recenseamento da população não recebeu muita resistência, porém em forte contraste com isso o debate social em torno dele era enorme. Além disso, afóra de um debate acalorado, o ato também foi levado perante os tribunais alemães, em última análise, vindo antes do Tribunal Constitucional alemão. A decisão deste tribunal acabou por confirmar o objetivo do censo populacional, mas exigiu salvaguardas processuais e organizacionais adicionais para os direitos fundamentais dos cidadãos. O censo populacional, no entanto não foi interrompido, mas adiado até um novo ato que permitiria que o censo da população fosse aprovado mais tarde, em 1987. No entanto, o julgamento do tribunal foi muito importante. Em seu julgamento, o tribunal afirmou que o direito à autodeterminação da informação era um direito constitucional fundamental. Além disso, era a implementação de um direito geral da personalidade, que era constituído pela proteção da dignidade e, por outro lado, a proteção pessoal em geral da liberdade. Ademais, o direito garantiu a capacidade do indivíduo de decidir ou determinar a liberação e o uso de seus dados pessoais (RUARO, 2020, p. 236-238).

Portanto, o conceito de autodeterminação informativa redimensionou o debate sobre dados pessoais em torno do titular de dados, que deve possuir controle sobre como suas informações pessoais são coletadas, armazenadas e compartilhadas (PESSOA, 2023, p. 43). Por

fim, a quarta geração de legislações de dados, vivenciada até os dias de hoje, leva em consideração as mais recentes, efetivas e perniciosas formas de coleta de dados contemporâneas. Tais normas buscam fortalecer o indivíduo frente às instituições coletoras de dados, reconhecendo que não estão nas mesmas condições para simplesmente negociar com elas. Assim, o consentimento deve ser, no mínimo, livre, informado, inequívoco, explícito ou específico, bem como deve estar presente em todas as fases do processamento (LUGATI; ALMEIDA, 2020, p. 6).

O Conselho Europeu, nas Convenções 108 e 108+, dispõe sobre o fluxo transfronteiriço de dados, e mencionam a necessidade da existência de um propósito legítimo para o tratamento de dados e uma base legal para o processamento (RUARO, 2020, p. 241). Pela influência das convenções, a Diretiva 95/46/CE do Parlamento Europeu, de 1995, foi responsável por estruturar um modelo europeu unificado, no que diz respeito à proteção das pessoas singulares, ao tratamento de dados pessoais e à livre circulação de tais dados entre os Estados-membros da União Europeia (LUGATI; ALMEIDA, 2020, p. 7). Dessa forma, em 2016, revogando a Diretiva 95/46/CE, publica-se o conhecido Regulamento Geral de Proteção de Dados Pessoais, ou RGPD.

Em que pese o assunto seja explorado em mais profundidade nos capítulos posteriores, cumpre referir um breve histórico das legislações brasileiras de dados. Além da já referida disposição constitucional, a Carta Magna de 1988 também dispôs sobre o *habeas data*, remédio constitucional impetrado para assegurar o conhecimento de informações pessoais relativas ao impetrante (BRASIL, 1988). Ademais, o Código de Defesa do Consumidor, em 1990, dispõe em seu art. 43 que todas as informações constantes em cadastros, fichas, registros e dados relativos ao consumo, em como suas fontes, serão acessíveis ao consumidor, de forma clara (BRASIL, 1990). O Código, todavia, se inscreve mais em uma tradição geral de regular bancos de dados. Em seu art. 21, o Código Civil, de 2002, traz que a vida privada da pessoa natural é inviolável, podendo o juiz adotar as providências necessárias para sustar tal violação (BRASIL, 2002).

Em 2011, surge a lei nº 12.414, ou Lei do Cadastro Positivo. Para alguns autores, a lei é relevante na medida em que consolida o consentimento como necessário para o tratamento de dados de consumidores, disposição ausente no CDC (LUGATI; ALMEIDA, 2020, p. 11). Posteriormente, o Congresso Nacional aprovou a lei nº 12.965/2014, criando o Marco Civil da *Internet*, dispondo sobre os princípios basilares para o uso da *Internet* no Brasil (PESSOA, 2023, p. 49). Não obstante ainda carecesse de uma regulação específica sobre a proteção de dados, o Brasil reagiu aos escândalos de espionagem revelados por Edward Snowden, dentro



da Agência Nacional de Segurança do Estados Unidos, através do Marco Civil da *Internet*. O diploma constitui também um afastamento do ordenamento jurídico nacional da ideia de regular o uso da *Internet* por meio de leis penais, solução que se mostrava potencialmente lesiva aos avanços tecnológicos à época (LUGATI; ALMEIDA, 2020, p. 12).

Em 2018, foi aprovada no Poder Legislativo a redação final do Projeto de Lei nº 4.060/2012, e sancionada a Lei nº 13.709, ou Lei Geral de Proteção de Dados Pessoais (LGPD), embora não tenha entrado imediatamente em vigor. A discussão balizadora da LGPD se deu na esteira da aprovação do Regulamento Geral de Proteção de Dados Pessoais (RGPD), com a submissão em 2016, por parte do Poder Executivo, do Anteprojeto de Lei nº 5.276/2016, apensado ao já referido projeto. A LGPD trouxe diversos princípios que orientam a exploração e o tratamento de dados pessoais, dispondo exaustivamente sobre o consentimento e os mecanismos de fiscalização e proteção do titular de dados. Dessa forma, representa o estado da arte da regulação da proteção de dados no Brasil.

### 3. LEI GERAL DE PROTEÇÃO DE DADOS E A EUROPEIZAÇÃO NORMATIVA

Em que pese a Lei Geral de Proteção de Dados brasileira ser hoje a maior referência legislativa nacional em termos de proteção de dados, sua elaboração não foi livre de influências externas. Para além do histórico internacional das regulações trazido anteriormente, a LGPD precisa ser inserida no complexo contexto de interesses nacionais e internacionais do qual se originou.

Dessa forma, este capítulo pretende pormenorizar as relações e a sequência de eventos que resultou na elaboração da LGPD. Primeiramente, define-se o fenômeno da influência regulatória europeia a partir do Regulamento Geral de Proteção de Dados Pessoais. Em um segundo momento, busca-se averiguar a ocorrência desse fenômeno em relação à LGPD, e, sendo a resposta positiva, em que medida essa influência transparece no processo e na redação da lei brasileira.

#### 3.1. EUROPEIZAÇÃO NORMATIVA E O RGPD

O referido Regulamento Geral de Proteção de Dados Pessoais (RGPD) europeu, de 2016, aplicável diretamente a todos os países-membros da União Europeia a partir de 2018, é uma legislação paradigma em termos de proteção de dados. Dentre os direitos garantidos pelo Regulamento está a proteção mais rigorosa dos dados considerados “sensíveis”, o direito de acesso e correção, o direito ao esquecimento, à portabilidade dos dados, entre outros (PESSOA, 2023, p. 44). Todavia, o Regulamento não impactou tão somente os países sujeitos à sua aplicação direta.

Em 2014, a Corte de Justiça da União Europeia aplicou dispositivos normativos europeus em face de um provedor de serviços estrangeiro, no caso *Google Spain*. Apesar da Google ser uma empresa estadunidense, a sanção se justificou em razão da multinacional ter estabelecimentos em solo europeu, e ao titular de dados foi reconhecido seu “direito de ser esquecido” (RYNGAERT; TAYLOR, 2019, p. 5-6). À época, já se discutia a extraterritorialidade da legislação europeia que, em determinadas temáticas, acabava gerando efeitos ao redor do mundo, influenciando na regulação exercida por diversos países. O RGPD veio dar ainda mais credibilidade a essa hipótese.

O Efeito Bruxelas, tese desenvolvida por Anu Bradford, é um fenômeno de globalização regulatória unilateral, no qual uma jurisdição é capaz de “exportar” padrões legislativos para outros países, como uma forma própria de exercício de *soft power* (BRADFORD, 2012, p. 3-

4). Como o nome sugere, o fenômeno é verificado principalmente a partir da atuação da União Europeia. De acordo com Bradford, sua materialização está limitada pelo preenchimento de algumas condições, dentre as quais o reconhecimento, por parte de grandes empresas, do benefício de adotar uma legislação global uniforme, ao invés de múltiplas. Da perspectiva de outros Estados, estes nada têm a ganhar travando uma competição regulatória com a União Europeia, de modo que a regulação unilateral envolve a jurisdição dominante impondo incentivos para o ajuste, seguida de uma “emulação relutante” dos participantes de mercado (BRADFORD, 2012, p. 9).

Ademais, um conjunto cumulativo de cinco fatores deve se manifestar para a ocorrência do fenômeno (GUNST; VILLE, 2021, p. 439). Inicialmente, a jurisdição externalizada deve possuir um mercado suficientemente grande, de forma que empresas multinacionais não possam prescindir das vantagens de lá atuarem. À época da consolidação das leis de dados vigentes, a União Europeia já constituía a maior economia do mundo, assim como a maior importadora de bens de serviços (BRADFORD, p. 11). Em segundo lugar, a capacidade regulatória para criar e reforçar padrões, diretamente ligada à existência de instituições fortes e bem consolidadas no âmbito internacional, como é o caso do Conselho da União Europeia, do Parlamento Europeu e da Comissão Europeia.

Em terceiro lugar, o contexto da jurisdição externalizante deve ser favorável às leis mais austeras, tendência verificada em países mais ricos, capazes de perseguir a minimização de riscos econômicos e consumeristas em detrimento da lucratividade de suas empresas. Em quarto lugar, o foco da regulação deve ser um mercado inelástico, ou seja, dificilmente movível em face de regulações mais austeras. Por esse motivo, a União Europeia tende a regular os mercados consumidores. Por fim, os bens e serviços alvo de regulação devem ser indivisíveis, em outras palavras, custosos ou impossíveis de serem regulados de forma específica em diferentes jurisdições (BRADFORD, 2012, p. 14-19).

Ainda, convém referir a diferenciação formulada por Bradford em relação à perspectiva *de facto* e *de jure*:

Deslindar os elementos determinantes da regulação unilateral globalizada explica por que a UE se tornou o regulador predominante do comércio global, e por que a UE pode exportar certas normas com sucesso e outras não. A UE tem o maior mercado interno do mundo, suportado por fortes instituições regulatórias. Negociar com a UE exige que empresas estrangeiras ajustem suas condutas ou produtos para padrões europeus – que frequentemente representam os padrões mais exigentes – ou renunciar o mercado europeu completamente. Raramente opta-se pelo segundo. Além disso, empresas não podem evitar normas da UE movendo os objetos de regulação para outra jurisdição pois a UE primariamente regula mercados consumidores inelásticos, ao invés de mercados de capitais mais elásticos. Por mais que a UE regule apenas seu

mercado interno, empresas multinacionais muitas vezes têm um incentivo para padronizar sua produção global e aderir a uma única regra. Isso converte a norma da UE em uma norma global – o “Efeito Bruxelas de facto”. Finalmente, depois que essas empresas centradas em exportação ajustaram suas práticas de negócios para adaptar-se aos estritos padrões europeus, elas geralmente têm o incentivo de praticar lobby em seus governos locais para adotar os mesmos padrões em um esforço de equalizar as condições contra seus competidores locais não centrados em exportação – o “Efeito Bruxelas de jure” (BRADFORD, 2012, p. 5-6). [tradução nossa].

Dessa forma, a perspectiva *de facto* trata da convergência de empresas e outros atores internacionais à uniformidade de regulação, enquanto a *de jure* dá conta da adoção de legislações similares por esses agentes, em âmbito doméstico (MUCHIUTI, 2022, p. 24). Dentre as temáticas nas quais a União Europeia é capaz de exercer regulação unilateral estão as leis antitruste, as normas referentes à saúde e produtos químicos, a proteção do meio ambiente, a segurança alimentar e a privacidade (BRADFORD, 2012, p. 19-32).

No que tange especificamente à proteção de dados, em que pese a ocorrência do Efeito Bruxelas não constitua necessariamente uma ação coordenada e planejada pela União Europeia, a elevação da privacidade ao rol de direitos fundamentais não permite discricionariedade regulatória por parte da mesma (RYNGAERT; TAYLOR, 2019, p. 6). Ou seja, na ausência de uma cláusula limitadora de jurisdição na Carta dos Direitos Fundamentais da União Europeia, o órgão está vinculado por suas próprias normas a agir, dentro de suas capacidades, influenciando o tratamento de dados além de suas fronteiras, de forma a proteger os direitos do titular de dados europeu.

Nesse contexto, a União Europeia parece ter adotado, em certa medida, a condição de reguladora internacional de proteção de dados (RYNGAERT; TAYLOR, 2019, p. 09). Para além das sanções pontuais às *big techs* anteriormente referidas, o Parlamento Europeu aprovou recentemente dois pacotes legislativos relevantes: o *Digital Service Act* (DSA), e o *Digital Markets Act* (DMA). O DSA busca contrapor a grande quantidade de conteúdo ilegal que circula na *Internet*, exigindo maior transparência por parte das plataformas e limitação do uso de determinados dados pessoais para customização de anúncios. O DMA, por sua vez, busca promover condições equitativas de concorrência entre plataformas digitais de diferentes portes, combatendo a concentração de produtos e serviços por parte de empresas maiores. Ambos os diplomas possuem aplicação assimétrica, ou seja, levam em consideração o tamanho das plataformas submetidas às normas, e estipulam sanções graduais conforme a capacidade que a empresa teria de dar adequado cumprimento às exigências das regulações (KIRA; COUTINHO; GONÇALVES, 2022).

Não obstante, o mais notório exemplo da influência regulatória europeia no âmbito da

proteção de dados internacional é o próprio RGPD. A normativa abrange os agentes de tratamento situados na União Europeia, e quem venha a tratar dados pessoais dos residentes no território da União Europeia, estipulando que todas as empresas que coletam, armazenam e processam dados pessoais desses titulares devem se submeter à norma, ficando vedado o tratamento de dados em países que não possuem proteção equivalente (UE, 2016, art. 44). Dessa forma, em uma manifestação dos aspectos *de facto* e *de jure* do Efeito Bruxelas, empresas estrangeiras passaram a ajustar suas práticas de acordo com o RGPD, e outras jurisdições adotaram modelos legislativos semelhantes (MUCHIUTI, 2022, p. 23-24).

No que tange ao efeito *de facto*, diversas *big techs* adotaram disposições dos RGPD em seu funcionamento interno. A Apple, em seu portal de privacidade, compromete-se com diversos padrões do RGPD, reproduzindo quase por completo o art. 6º da normativa no que diz respeito às hipóteses do tratamento de dados (APPLE, *Privacy Policy*, 2023). Da mesma forma, a empresa adota, implícita ou explicitamente, diversos princípios do regulamento. Plataformas como Google e Facebook também incorporam os princípios e a terminologia do regulamento em suas políticas de privacidade e termos de uso, a despeito do emprego de soluções mais regionalizadas, especialmente no caso da última (GUNST; VILLE, 2021, p. 442-447).

Em relação à prática de *lobby* para a adoção de legislações compatíveis, resultando no aspecto *de jure*, pertine o caso da Lei de Privacidade do Consumidor da Califórnia, ou CCPA, aprovada em 2018, nos Estados Unidos. Em que pese ser uma lei estadual, a normativa impõe observância ao princípio da transparência, maior garantia do acesso do consumidor aos seus direitos e diversas incumbências aos responsáveis pelo tratamento de dados (PESSOA, 2023, p. 47). É relevante que esta seja a primeira lei abrangente de proteção de dados estadunidense, e que possua semelhanças notáveis com o RGPD, haja vista a diferente tradição regulatória dos Estados Unidos *vis à vis* da União Europeia.

Em análise do processo legislativo da CCPA, Gunst e Ville aportaram uma leitura nuançada:

Depois de avaliar o impacto do RGPD na política de privacidade de algumas companhias californianas, há evidência significativa para concluir que o Efeito Bruxelas *de facto* está presente. Não obstante, também há evidência para concluir que não está *sempre* presente. A explicação para essa afirmação a princípio contraditória pode ser bastante simples: algumas partes do RGPD são indivisíveis, outras não. Portanto, não é correto afirmar que a legislação de proteção de dados europeia como um todo goza do Efeito Bruxelas, mas sim que provisões individuais se beneficiam (...). No que diz respeito à conexão entre o efeito *de facto* e *de jure*, i.e., esforços de *lobbying* para alinhar o quadro californiano com o RGPD, há também evidência significativa. Uma observação interessante aqui é que Apple e Google apenas praticaram *lobby* para a inclusão de conceitos do RGPD na CCPA aos quais eles já haviam se adequado de qualquer forma (...). Por fim, existem apenas poucas evidências

concretas para a ocorrência do Efeito Bruxelas *de jure*. De fato, existem mais evidências significativas do contrário, nas quais o governo californiano explicitamente rejeitou alinhamento com o RGPD. A evidência mais clara diz respeito à rejeição da criação de um porto seguro (para a aplicação do RGPD). Considerando que tal porto seguro faria da CCPA (parcialmente) irrelevante para companhias que já respeitam o RGPD, sua inclusão teria sido extremamente notável (...) A evidência contrária, portanto, em nossa opinião, não desqualifica a conclusão de que o Efeito Bruxelas de fato teve papel significativo na adoção da CCPA (GUNST; VILLE, 2021, p. 457-458). [tradução nossa].

Dessa forma, é possível verificar a influência do Efeito Bruxelas, em ambos os seus aspectos, na adoção da CCPA estadunidense. Outros países desenvolvidos também passaram por processos semelhantes, como foi o caso do Japão, com a modificação do *Act on the Protection of Personal Information* (APPI), em 2021 (MUCHIUTI, 2022, p. 23). Ademais, é possível atribuir a adoção de normas específicas sobre proteção de dados às demandas de ingresso na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), bloco econômico composto por diversos países ricos. A OCDE editou, ainda na década de 1980, as Diretivas sobre Proteção da Privacidade e Fluxo de Dados Transfronteiriços, e atualizou-as em 2013, de forma que recomendam que os países membros adotem legislações apropriadas, incluindo princípios como a limitação da coleta, qualidade dos dados, finalidade, entre outros. Trata-se de um grupo que o Brasil deseja aderir (BIONI, 2021, p. 59-64).

Em seu texto, Bradford não categoriza a regulação unilateral do Efeito Bruxelas como boa ou ruim. A depender das circunstâncias internas do país, a influência europeia poderá sobrepor legislações mais ou menos funcionais que o RGPD (BRADFORD, 2012, p. 64). Ainda assim, argumenta-se que o poder dado às instituições europeias para determinar indiretamente o que empresas estrangeiras podem fazer é problemático para os envolvidos, mas é especialmente preocupante a hipótese de uma legislação europeia preencher o vazio legislativo de um país, impedindo-o de chegar às suas próprias soluções normativas.

### 3.2. A LGPD E O RGPD

A influência do Regulamento Geral de Proteção de Dados europeu na Lei Geral de Proteção de Dados Pessoais brasileira não é um ponto controvertido para a doutrina. Afinal, o Regulamento é aplicado a qualquer empresa que ofereça bens ou serviços e que colete dados de residentes da União Europeia, englobando as *big techs*. Toda empresa ou organização que não pagar os custos de conformidade com o RGPD está incapacitada de tratar dados de residentes de qualquer um dos Estados-membros; por sua vez, a Comissão Europeia impõe que país para o qual se transfere dados assegure um nível de proteção adequada, qual seja,

semelhante ao Regulamento. Dessa forma, é compreensível que exista uma tendência à uniformização regulatória (FACHIN, 2022, p. 1.549-1.569).

Não obstante, faz-se necessária uma análise particular do caso brasileiro, para determinar em que medida o Efeito Bruxelas se manifestou na legislação de proteção de dados nacional. Primeiramente, a verificação do aspecto *de facto* deve decorrer de uma análise do processo legislativo da LGPD, comprovada a ocorrência de *lobby* para a aprovação da lei. Em um segundo momento, passa-se à comparação dos dois textos normativos, determinando em que medida o efeito *de jure* se faz presente.

Já em meados dos anos 2000, discussões internacionais no âmbito do Mercosul suscitaram a necessidade de uma norma comum de proteção de dados aos países do bloco. Ainda que as negociações não tenham ganhado tração, mobilizaram iniciativas dentro do Ministério da Justiça para a confecção da minuta do Anteprojeto de Lei de Proteção de Dados Pessoais, submetido à consulta pública no final de 2010. À exceção de pareceres opinativos emitidos principalmente pelo terceiro e segundo setor (9 associações empresariais e congêneres, 4 empresas), as discussões iniciais tiveram pouco efeito (BIONI, 2021, p. 21-23). Em 2012, foi apresentado na Câmara dos Deputados o Projeto de Lei nº 4.060/2012, pelo Deputado Milton Monti, contando com 25 artigos (MUCHIUTI, 2022, p. 25).

O projeto fica em segundo plano até 2015, quando é desarquivado por influência da discussão e do trâmite do RGPD. Com uma nova versão do Anteprojeto, o Ministério da Justiça submete à outra consulta pública, com mais participação multissetorial (BIONI, 2021, p. 24-25). Em 2016, o Anteprojeto de Lei nº 5.276/2016 foi submetido em regime de urgência pelo Poder Executivo, e apensado ao PL nº 4.060/2012 (PESSOA, 2023, p. 50). O Deputado Orlando Silva foi indicado para a relatoria do projeto por articulação da chamada Coalizão Direitos na Rede, formada por entidades da sociedade civil, sinalizando a maturação dos debates. A Comissão Especial formada na Câmara promoveu diversas audiências públicas (BIONI, 2021, p. 29).

Apesar das discussões qualificadas, ao final de 2017, ainda não havia perspectiva de aprovação da lei, de forma que foi necessária uma conjuntura favorável composta por diversos atores para sua concretização. Bioni assim a descreve.

Resumidamente, essa conjuntura favorável pode ser atribuída a, pelo menos, quatro fatores de destaque, que ocorreram paralelamente no Brasil e no mundo e concorreram para a formação de um cenário fortemente propício à aprovação de uma lei geral de proteção de dados brasileira. Foram eles: i) o escândalo Cambridge Analytica, que precipitou um debate por vezes restrito a círculos específicos para a grande mídia e o grande público; ii) a entrada em vigor, em maio de 2018, do Regulamento Geral de

Proteção de Dados (RGPD) europeu, que acirrou a necessidade de maior segurança jurídica quanto ao tratamento de dados no Brasil; iii) o desejo expresso do Brasil ingressar na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que exige, como boa prática, a regulamentação de uso de dados pessoais, assim como um órgão supervisor independente e autônomo; e, por fim, iv) uma articulação interna à Câmara dos Deputados para a aprovação das alterações na Lei do Cadastro Positivo, que envolvia a aprovação da Lei Geral de Proteção de Dados como condição indispensável (BIONI, 2021, p. 32)

Nestes termos, o relator da comissão emitiu parecer em 24 de maio de 2018, evidenciando a mobilização necessária por parte do setor privado:

Importante pontuar que as propostas se inserem em um contexto mundial, portanto, maior, em que legislações nacionais são introduzidas em cada país, de forma a tratar da questão dos dados pessoais e garantir a proteção das pessoas de maneira harmônica. Ao mesmo tempo, a construção de um arcabouço similar entre os países gera um ambiente propício aos negócios, principalmente globais, oriundos do manuseio de dados (...) Grande fonte de inspiração para os projetos advém do arcabouço europeu (...) Em 2016, o sistema europeu foi revisado com a aprovação do Regulamento no 679, de 2016, do Parlamento Europeu e do Conselho, de 27/04/2016, que trata da proteção das pessoas naturais com respeito ao processamento de dados pessoais e ao livre movimento desses dados (...) Esse ponto, de a legislação do país estar de acordo com a legislação europeia, é extremamente pertinente neste julgamento, pois indica, como questão de fundo, a atratividade comercial do setor de TIC (Tecnologia da Informação e das Comunicações) dos países. Em tempos de computação em nuvem, um país que atenda à legislação europeia possui condições de atrair processamento de dados daquele bloco. E atrair o tratamento de dados implica não só a possibilidade de instalação de data centers, mas das próprias empresas de TIC, incluindo as gigantes ponto com. Por isso, a necessidade de o Brasil possuir, sem abrir mão de suas especificidades e soberania, uma legislação harmônica com o mundo e com os principais blocos organizados, como a União Europeia (BRASIL, 2018).

Ao longo dos debates, existiam dissensos entre a sociedade civil, defensora de uma norma mais protetora, e outros setores alinhados às empresas que deveriam implementar a lei. Concessões tiveram de ser feitas dos dois lados (MUCHIUTI, 2022, p. 31). Em 13 de julho de 2018, foi lançado pela Brasscom o Manifesto de Aprovação da Lei de Proteção de Dados, no qual 80 signatários, principalmente empresas de diversos ramos e associações representativas de entes do setor privado, se uniram com o objetivo comum de pressionar o Senado Federal (BIONI, 2021, p. 19).

O manifesto reproduz claramente muitos dos motivos já expostos anteriormente nas discussões do projeto, seja no que diz respeito ao atraso do Brasil em relação a outros países, seja na necessidade de atrair investimentos (BRASSCOM, 2018). De acordo com Muchiuti:

[...] na tramitação do PL há a recorrente presença dos argumentos de que o Brasil deveria adotar a normativa como forma de adequação, vez que estaria atrasado em comparação com as legislações de outros países que já possuíam diplomas visando à proteção de dados pessoais (dentre eles, a UE), reduzindo assim as chances de obtenção de investimentos financeiros internacionais, bem como precisaria de uma



regulamentação harmônica com o RGPD, já que a normativa europeia não permite a transferência internacional de dados para países que não possuem o mesmo nível de segurança, o que, portanto, impactaria a atratividade econômica do setor de Tecnologia da Informação e das Comunicações brasileiro. Na tramitação do PL, há também evidências de intensa participação do setor privado - por meio das entidades citadas no quadro acima e outras para além das mencionadas - seja por meio de uma representação direta, como é o caso do Facebook e do Mozilla, seja por meio de associações representativas de diferentes segmentos, como a ABAP, a ABEMP e a BRASSCOM (MUCHIUTI, 2022, p. 32-33).

Pouco depois, a lei foi aprovada de forma unânime na Câmara e no Senado, restando a necessidade de sanção ou veto presidencial. Todavia, a autoridade encarregada de fazê-lo era de um governo diverso do que havia elaborado o Anteprojeto, de forma que novos debates se fizeram necessário, e a concordância temporária entre os setores da conjuntura anterior ficou prejudicada. Nessa fase, houve a supressão do modelo da Autoridade Nacional de Proteção de Dados como estrutura de agência reguladora por um modelo de órgão vinculado à Presidência da República (BIONI, 2021, p. 35-37). Não obstante, a LGPD entrou em vigor plenamente em setembro de 2020 sem outras alterações substanciais, e a breve análise empreendida no processo legislativo evidencia a ampla participação do setor privado ao longo de seu trâmite, bem como o aspecto *de facto* do Efeito Bruxelas.

No que se refere ao Efeito Bruxelas *de jure*, faz-se necessária uma análise mais detida dos diplomas normativos. Inicialmente, aponta-se que ambos decorrem de técnicas e tradições legislativas diversas, sendo o RGPD composto por 173 “considerando” e 99 artigos, e a LGPD formada por 65 artigos. Enquanto o RGPD incide sobre diversos países, a LGPD incide apenas no território brasileiro, ressalvado o fato de que ambos tutelam o tratamento de dados localizados fora de suas jurisdições, pela própria natureza transnacional da matéria (FACHIN, 2022, p. 1.558-1.559). Distinções à parte, os textos apresentam notáveis semelhanças. Para fins de brevidade, serão analisados alguns pontos basilares, divididos em princípios, bases legais e disposições sobre controle e responsabilização.

Com relação aos princípios do RGPD, pode-se argumentar que estes decorrem da tradição internacional dos *Fair Information Practice Principles*, em desenvolvimento desde os anos 70, nas primeiras legislações de proteção de dados (BIONI, 2021, p. 374-377). Destes, o RGPD abarca os princípios da necessidade (art. 5º, 1.a), licitude (art. 5º, 1.a), proporcionalidade (art. 5º, 1.a), transparência (art. 5º, 1.a), finalidade (art. 5º, 1.b), minimização dos dados (art. 5º, 1.c), exatidão (art. 5º, 1.d), atualidade (art. 5º, 1.e) e responsabilidade (art. 5º, 2) (UE, 2016).

O legislador brasileiro, por sua vez, reproduziu na LGPD, em seu art. 6º, todos os princípios constantes do RGPD, guardadas as proporções. Prevê, além dos princípios anteriormente citados, o livre acesso (art. 6º, IV), a segurança (art. 6º, VII), a prevenção (art.

6º, VIII) e a não discriminação (art. 6º, IX). Destaque especial pode ser dado à boa-fé, posicionada no *caput* do art. 6º, que remete à tradição civilista brasileira de forma particular (BRASIL, 2018). Dessa forma, pode-se concluir que as duas legislações apresentam bases principiológicas comuns, com a legislação brasileira ampliando alguns dos ditames presentes no regulamento europeu.

O processamento de dados somente é adequado se estiver de acordo com alguma base legal, sendo o consentimento a mais conhecida (RUARO, 2020, p. 243). O RGPD elenca 6 bases legais, em seu art. 6º, quais sejam: consentimento, execução de contrato, obrigação jurídica, defesa de interesses vitais, exercício de funções de interesse público e legítimo interesse (UE, 2016). A LGPD trouxe, além de todas as bases previstas no diploma europeu, quatro bases adicionais em seu art. 7º: realização de estudos por órgãos de pesquisa, exercício regular de direitos em processo judicial, tutela da saúde e proteção do crédito (BRASIL, 2018).

Convém pontuar que a hipótese do legítimo interesse ensejou discussões ao longo do processo legislativo da lei brasileira. Os primeiros modelos submetidos em nada tratavam dessa base legal, prevalecendo o consentimento como hipótese legitimadora principal, abordagem que era coerente com outras legislações internas, como o Marco Civil da *Internet*. De acordo com Bioni, a inclusão do legítimo interesse data de 2015 de forma hierarquicamente equivalente ao consentimento e sinalizava uma necessidade de adequação às legislações internacionais:

De um lado, empresas como Claro, Vivo, Sky e associações empresariais como Febraban e Brasscom, dentre outras, defenderam existir uma “fadiga do consentimento”, isto é, um peso desproporcional sobre o próprio titular que deveria decidir sobre o tratamento de seus dados em todas hipóteses. Assim, as empresas apontaram o legítimo interesse como hipótese legal facilitadora do tratamento de dados em situações nas quais não haveria impactos indevidos sobre os direitos dos indivíduos, sem, entretanto, entrar em considerações mais aprofundadas sobre esses direitos ou sobre os interesses dos titulares. Outras contribuições, como a de Marcel Leonardi, ressaltaram o fato de o legítimo interesse integrar a legislação europeia sobre o tema desde 1995, de forma que se criaria um descompasso e um atraso caso o Brasil optasse por não seguir esse mesmo caminho. Representantes de ONGs e da academia, entidades como ITS Rio e o Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação (GPOPAI) estressaram o debate (...) Tais contribuições da sociedade civil reverberaram nas escolhas do Ministério da Justiça, uma vez que, apresentado o texto pós-consulta pública, ele trazia, para além da previsão do legítimo interesse como uma base legal para o tratamento de dados pessoais, também uma série de parágrafos que tornaram essa previsão mais robusta e equilibrada (...) A disputa sobre consentimento e legítimo interesse demonstra (i) a força de um consenso entre setores tradicionalmente antagônicos sobre a necessidade de superação da hierarquia do consentimento, (ii) a existência de discordâncias sobre o conteúdo da previsão do legítimo interesse, se mais “protetiva” dos interesses do titular, ou menos, desde a segunda consulta pública até o final do processo legislativo; (iii) o fato de que, a despeito do forte multissetorialismo ao longo de toda a trajetória da lei, a coalizão tática, de fato, se deu apenas em um momento específico e bastante restrito no tempo (BIONI, 2021, p. 42-45)

Dessa forma, extrai-se a manifestação de ambos os aspectos do Efeito Bruxelas mesmo em análise isolada de uma das bases legais. Ademais, tece-se uma consideração em relação ao tratamento de dados sensíveis em ambos os diplomas. O RGPD proíbe o tratamento de dados, exceto no caso de dados publicados pelo proprietário, ou dados sobre membros e ex-membros de fundações, associações ou organizações sem fins lucrativos para fins lícitos e de forma adequada. Nenhuma dessas exceções foram incorporadas ao LGPD, que prevê que os dados sensíveis podem ser tratados independentemente de consentimento do titular quando forem indispensáveis para exercício de funções pela administração pública ou para garantia de prevenção de fraude e segurança do titular na identificação e autenticação do registro em sistemas eletrônicos (RUARO, 2020, p. 244).

Por fim, algumas considerações gerais sobre controle e responsabilização. Ambos os diplomas instituem autoridades fiscalizadoras, seja o Comitê Europeu para a Proteção de Dados, no caso do RGPD, ou a Autoridade Nacional de Proteção de Dados Pessoais, no caso da LGPD. No workshop “Transferência internacional e o sistema de proteção de dados pessoais no Brasil: caminhos para decisões de adequação”, ocorrido no 11º Fórum da *Internet* no Brasil, realizado, em julho de 2021, pelo Comitê Gestor da *Internet* no Brasil (CGI.br), a importância da decisão de adequação pela União Europeia em favor da lei brasileira e o diálogo internacional sobre marcos jurídicos é sublinhada por uma representante da Autorização Nacional de Proteção de Dados (ANPD)<sup>2</sup>.

Da mesma forma, ambos dispõem sobre instrumentos de responsabilização do controlador, na forma do relatório de impacto à proteção de dados pessoais, descritos mais minuciosamente no RGPD. Na LGPD, em que pese não exista a mesma obrigatoriedade ou especificação, o relatório é descrito como “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (art. 5º, XVII). Um estudo conduzido pelo LGPD Acadêmico (2020) sistematizou a compatibilidade das atividades de gerenciamento de privacidade e proteção de dados entre ambos os diplomas. Concluiu-se que 65 das 83 atividades previstas no RGPD são reproduzidas no LGPD.

Assim, resta evidente a ocorrência do Efeito Bruxelas, em ambos os seus aspectos, em relação à legislação brasileira. O processo legislativo da LGPD foi permeado por intenso *lobby*

---

<sup>2</sup> [FIB11] Transferência internacional e o sistema de proteção de dados pessoais no Brasil. 1 vídeo (1h 37 min). Workshop publicado pelo canal NICBrvídeos. Disponível em [https://www.youtube.com/watch?v=NW\\_zyk8-f5Y&ab\\_channel=NICBrvídeos](https://www.youtube.com/watch?v=NW_zyk8-f5Y&ab_channel=NICBrvídeos). Acesso em: 16 nov. 2023.

do setor privado, para fins de melhor responder à aprovação do RGPD no cenário internacional. Da mesma forma, o diploma reproduz em diversos momentos as disposições do RGPD, ressalvadas distinções pontuais, tomando como base os mesmos fundamentos da legislação europeia em seu texto.

#### 4. A FUNÇÃO SOCIAL DAS *BIG TECHS*

Em um contexto de capitalismo de vigilância e europeização normativa, o titular de dados brasileiro se encontra em uma situação precária. É lícito questionar se as respostas normativas nacionais são coerentes com a realidade brasileira, haja vista atuar como coadjuvante no estabelecimento das lógicas às quais está sujeito.

Dessa forma, diante de toda a pesquisa realizada, o presente capítulo pretende tecer considerações acerca das perspectivas do titular de dados brasileiros. Inicialmente, são apontados os descompassos da legislação vigente com a realidade de um país emergente, e qual lógica de dominação ela contribui para reforçar. Por fim, busca-se conceituar uma alternativa jurídica emancipatória na forma da função social da empresa.

##### 4.1. INADEQUAÇÕES DA LGPD À REALIDADE BRASILEIRA: COLONIALISMO DE DADOS E MOTIVAÇÕES MERCADOLÓGICAS

Em que pese a LGPD represente um marco importante para a legislação brasileira, esta deve ser analisada face ao contexto econômico de sua concepção e à europeização normativa. Aqui, cabe ressaltar que o reconhecimento da ocorrência do Efeito Bruxelas não permite concluir que a União Europeia está engajada em uma espécie de imperialismo institucional, tampouco que o RGPD seja uma base inapropriada para edificar uma legislação de proteção de dados nacional. Da mesma forma, a participação do setor privado no processo legislativo da LGPD, por si só, não deslegitima suas intenções e seus avanços.

Todavia, parece ingênuo não reconhecer a posição subalterna adotada por um país emergente como o Brasil que, sujeito à lógica do capitalismo de vigilância imposto por empresas originárias de uma jurisdição estrangeira, adota um modelo de legislação difundido por outra potência estrangeira. Nesse contexto, a LGPD é sintomática desse processo complexo que condiciona países emergentes a uma posição de subserviência também em relação à tecnologia. A problemática da inadequação da LGPD para a realidade brasileira pode ser melhor explicitada pela ocorrência do chamado colonialismo de dados e pela análise de suas motivações mercadológicas.

Na condição de país sul americano, o Brasil está inserido no grupo de países localizados no chamado “Sul Global”, juntamente com o restante da América do Sul, África e Ásia. Tais países possuem em comum o fato de terem sido colonizados por países ricos e imperialistas em seu passado, promovendo, primeiramente, lutas *descoloniais* e, em um segundo momento,

*decoloniais*. Enquanto as primeiras representaram lutas políticas pela independência, travadas, em sua maioria, no século XVIII e XIX nas Américas, e após a Segunda Guerra Mundial na África e na Ásia, as lutas contra a *colonialidade* perpassam a superação dos mecanismos de dominação que persistem mesmo após a independência (CASSINO, 2021, p. 14-15). A colonialidade se mantém por mentalidades e relações de subordinação, bem como por uma visão etapista e eurocêntrica que desvaloriza outras culturas e saberes (SILVEIRA, 2021, p. 37).

Os estudos sobre colonialidade desenvolvidos no século XX no Brasil perpassam essencialmente dois grandes momentos, de acordo com Cassino. Primeiramente, as teorias evolucionistas/culturalistas da primeira metade do século que, embora reconhecessem o legado colonial português como pernicioso para o desenvolvimento da democracia brasileira, instituíram ideias hoje superadas, como a inexistência de racismo no Brasil por causa da miscigenação e concepções eurocêntricas de progresso. Por sua vez, a teoria da dependência, desenvolvida por autores como André Gunder Frank e Theotônio dos Santos, com forte influência marxista, sustenta que toda a modernidade dependeu da colonização das Américas, grandes fontes dos recursos necessários para a Revolução Industrial. Para além do Brasil, influenciam e constroem os estudos pós-coloniais autores como Frantz Omar Fanon e Aníbal Quijano (CASSINO, 2021, p. 21-26).

Para os autores pós-coloniais, a colonialidade é um dos principais elementos do padrão mundial de poder capitalista (SILVEIRA, 2021, p. 36). Por sua vez, o capitalismo de vigilância encontra suas condições de existência em um contexto de prevalência da doutrina neoliberal na economia mundial. O neoliberalismo, que assumiu diversas formas desde as primeiras utilizações do termo em meados do século XX, representa hoje uma doutrina ou modelo de intervenção mínima do Estado, em que todos os aspectos da vida são regulados pelo capital e pelo mercado. O Estado, na prática, acaba funcionando como um garantidor do sistema neoliberal, servindo para a manutenção de instituições financeiras ou mesmo operando como uma grande empresa (VIANNA, 2021, p. 126-127). O mercado está acima de todas as dimensões da vida, e a empresa é o centro gravitacional da sociedade. O modelo neoliberal consolida a colonialidade (SILVEIRA, p. 37-38).

Neste contexto se desenvolve o capitalismo de vigilância descrito por Zuboff, ou capitalismo de plataforma, na terminologia de Srnicek (SRNICEK, 2016). Uma nova forma de mercadoria ganha valor, os dados, mas somente para aqueles com a capacidade técnica de tratá-la. O titular produz dados em troca do uso das plataformas que, inobstante mostrassem grande potencial para fortalecer a comunicação entre as pessoas no início, parecem ter reforçado uma

postura individualista de cunho neoliberal através de suas práticas corporativas. Essa postura opera em detrimento da esfera pública e da possibilidade de soluções coletivas, vulnerabilizando a capacidade de resposta do titular. Dessa forma, “há uma ideologia que valoriza a individualidade ao mesmo tempo em que torna as pessoas invisíveis” (FORNASIER; KNEBEL, 2021, p. 1.010-1.011).

Todos os titulares de dados que desejem usufruir dos serviços prestados pelas *big techs*, essenciais para a vida moderna, devem se submeter a um regime de entrega de dados, independentemente da cultura, religião ou país de origem. Todos os dados são extraídos e utilizados, servindo de alguma maneira para o modelo de lucratividade exponencial empregado por essas empresas (ZUBOFF, 2021, p. 97). Todavia, os efeitos da implementação dessa lógica em países do Norte e do Sul são fundamentalmente diferentes, deixando explícita uma nova forma de colonialismo:

Em primeiro lugar, o Norte é produtor e exportador das tecnologias, beneficia-se dos lucros obtidos por suas empresas, recebe as remessas financeiras obtidas mundo afora. (...) Em segundo lugar, como mostrou Boaventura de Sousa Santos, criaram-se na época da colonização linhas abissais que dividiram o Velho Mundo (Europa) e o Novo Mundo (Américas). Tais linhas ainda se mantêm presentes na forma de pensar dos ocidentais, inclusive nas relações sociais, políticas e culturais. O pensamento moderno ocidental se baseia em um sistema de distinções – visíveis e invisíveis, sendo que as invisíveis fundamentam as visíveis. A realidade social estaria dividida entre dois universos: “deste lado da linha” e do “do outro lado da linha”. Ou seja, tudo o que está do outro lado da linha, fora do centro da modernidade ocidental, seria desconsiderado. O que acontece longe do centro é inexistente, uma vez que sequer é visto ou considerado. Não importa o que acontece na favela carioca, em Caracas ou em Bogotá. Ninguém vê. Na época do colonialismo histórico, temas centrais no debate político europeu sequer chegavam aos territórios coloniais. Os moradores das Américas não precisavam opinar, eles não existiam. Essa relação segue mais ou menos intocada na era do colonialismo de dados. Os produtores de tecnologia pouco se importam com os consumidores do Sul Global, salvo o recebimento de feedback para melhorias de seus próprios produtos ou com alguns nichos lucrativos. O que importa são os dados coletados. Os debates das antigas metrópoles foram substituídos pelo desenvolvimento, pela produção de equipamentos, por novos protocolos, pela pesquisa em ciência, tecnologia e inovação, know-how e pela propriedade intelectual (CASSINO, 2021, p. 29-30).

Assim, o colonialismo de dados é uma forma própria de dependência colonial surgida na era digital. Na lógica neoliberal, prevalece a seleção dos melhores produtos com os menores custos, inexistindo outros princípios relevantes. Da mesma forma, a possibilidade de investimento em soluções locais no capitalismo de dados, quando já existem soluções mais eficientes trazidas por países mais ricos, é uma “não-questão”. Sérgio Amadeu assim discorre sobre as questões mais importantes que acabam ofuscadas pela mentalidade colonial:

Primeiro, a dúvida sobre a crença de que as empresas e plataformas digitais são neutras e que não interferem em nosso cotidiano, exceto para nos servir. Segundo, a interrogação sobre a inexistência de consequências negativas locais e nacionais na utilização das estruturas tecnológicas das plataformas, uma vez que elas respeitariam os contratos. Terceiro, a avaliação de que as implicações sobre a coleta massiva de dados nos países centrais da plataformização tecnológica possuem os mesmos efeitos econômicos, políticos e socialmente moduladores que nos países periféricos. Quarto, a indagação sobre se seria possível apostar no avanço de uma inteligência computacional local, na soberania algorítmica e no conhecimento tecnológico como um bem comum livre (SILVEIRA, 2021, p. 36).

Particularmente relevantes são o terceiro e o quarto tópico elencados neste trecho. Sérgio Amadeu pontua que dificilmente os dados de titulares de países ricos são armazenados e tratados fora de seus países. O pretexto para tal proibição é a manutenção de uma superioridade tecnológica e geopolítica, bem como o reconhecimento da necessidade de uma segurança nacional que, nada obstante, nem mesmo é considerada no que tange aos países periféricos. No âmbito das regulações, seria inimaginável que algum país ou conglomerado sul americano pudesse estabelecer as mesmas condições de tratamento de dados que a União Europeia exige internacionalmente, por exemplo. Ademais, enormes verbas oriundas de publicidade percorrem o mesmo caminho que o fluxo de dados, dos países periféricos para os grupos que controlam as tecnologias, e a inteligência local fica paralisada diante do ordenamento neoliberal com as teias de colonialidade que “sustentam a posição de eterno dependente das tecnologias criadas na matriz” (SILVEIRA, 2021, p. 48-49).

À luz do contexto neoliberal, as motivações mercadológicas da LGPD restam evidenciadas. Como já analisado anteriormente, o processo legislativo da norma contou com forte *lobby* do setor privado, e uma argumentação baseada nos potenciais investimentos que poderiam ocorrer no país. De acordo com o manifesto da Brasscom, o Brasil estaria dando um passo para “proporcionar um ambiente de negócios seguro que potencialize a atração e materialização de investimentos na ordem de R\$ 250 milhões (Brasscom e Frost & Sullivan) em tecnologias de transformação digital até 2021” (BRASSCOM, 2018). As manifestações dos relatores, conforme já exposto, refletem preocupações semelhantes, sejam na ordem de “atualizar” o Brasil em relação ao modelo legislativo internacional, ou atrair investidores.

Assim, torna-se evidente a finalidade do modelo normativo adotado pelo Brasil via Efeito Bruxelas. Para Fornasier e Knebel, é essencial a compreensão de que regulamentos como o RGPD nascem não apenas para proteger o titular dos excessos da exploração de dados, mas para legitimá-la (FORNASIER; KNEBEL, 2021, p. 1.023). A criação de legislações desse tipo ilustra a institucionalização do capitalismo de vigilância. Tais normas consolidam o papel do Estado em um contexto neoliberal, qual seja, garantem as condições para a exploração



capitalista por parte das grandes empresas. Normas que legitimam o mercado de dados podem ser particularmente inadequadas para países periféricos, materialmente menos capazes de assegurar a proteção de dados de seus titulares.

Como o RGPD, a LGPD elege a autonomia privada no ato do consentimento como principal condição para o tratamento de dados. A despeito da existência e discussão de outras bases legais, o consentimento segue sendo a “pedra de toque” da norma. Contudo, o condicionamento dessa operação ao simples consentimento, ainda que livre, informado e inequívoco, qualifica o ato de disposição dos dados como uma mera transação (FORNASIER; KNEBEL, 2021, p. 1.017-1.018). Com isso, ignora-se a imensa disparidade entre as partes contratantes. Conforme já referido anteriormente, as *big techs* são empresas bilionárias, responsáveis por uma boa parcela dos avanços tecnológicos, que empregam sistemas de coleta de dados e algoritmos obtusos, restando o titular em uma condição de hipossuficiência *sui generis* mesmo no que se refere à relação de consumo.

A consolidação da extração de dados em um nível estrutural depende da ubiquidade dos serviços prestados pelas *big techs* e do aprofundamento da assimetria informacional entre titular de dados e empresa:

A assimetria informacional é o fator estrutural determinante dessa economia dos dados, justamente pela profunda desigualdade entre a capacidade de gerir e processar dados entre os usuários, titular de dados pessoais, e quem os controla, as *big techs* (...) só é possível com tecnologias de apropriação privada das corporações informacionais, em que a lógica do extrativismo de dados ocorre sob um consenso algoritmo forjado nos escritórios dessas empresas, sob princípios considerados “*bons para todos*”. O titular dos dados pessoais queda-se refém de um estrutura social que lhe deixa restrito ao papel de rendição de seus dados, mascarada de voluntariedade, ou o ostracismo que impossibilita o trabalho ou lazer (FORNASIER; KNEBEL, 2021, p. 1.012).

Dessa forma, quanto maior a assimetria técnica, menores são as condições fáticas de um consentimento real e informado, subsistindo a compreensão ficta das consequências do tratamento de dados e o incentivo a aderir. A assimetria informacional facilita uma mentalidade de alienação técnica, na qual existe uma “ignorância ativa sobre como funcionam as redes de criação, desenvolvimento e uso de tecnologias, na fé da completa ausência de importância de se conhecer e dominar localmente os processos tecnológicos” (SILVEIRA, 2021, p. 45). Passa Fornasier e Knebel, essa é a contradição da proteção de dados:

Por um lado, expõe a importância da autonomia privada, enquanto que, de outro, entende que os consumidores usuários estão em posição extremamente frágil nas suas relações para com as *big techs*. A imposição da economia política de vigilância restringe essa autonomia privada ao ato de disposição de seus dados pessoais a serem controlados por máquinas alheias e inacessíveis, dessa forma. O consentimentos como

afirmação dos direitos relativos aos dados digitais possui uma natureza controversa, justamente porque intenta consagrar liberdade e autonomia privada em um cenário de profunda desigualdade na gestão de dados - tendo em vista a assimetria de infraestrutura e conhecimento acerca da ciência de dados e da interpretação de dados massivos na era do *big data* - principalmente no que se refere ao mais recente aprendizado de máquinas e inteligência artificial. Sendo assim, no tocante a esse papel central da liberdade individual e da possibilidade formal que a LGPD sugere ser possível materialmente no campo do consentimento, questiona-se o consentimento sobre formas de análise de utilização de dados que seres humanos sequer conseguem conceber (FORNASIER; KNEBEL, 2021, p. 1.018).

Portanto, o consentimento mostra-se insuficiente na medida em que o titular não é nem mesmo capaz de compreender as tecnologias de coleta e como seus dados serão tratados. Tais processos tornam-se ainda mais opacos e intangíveis com a existência de uma barreira cultural, diferença linguística, carência de recursos e escassez de meios de resposta. Dessa forma, o titular de dados será sempre hipossuficiente e vulnerável em relação às *big techs*, mas o titular de dados em um país emergente, como o Brasil, será praticamente indefeso.

Há contenciosidade também em relação às outras bases legais elencadas pela LGPD. A título de exemplo, traz-se o caso dos corretores de dados, mercado que atua de forma particularmente opaca. Os corretores de dados, ou *data brokers*, são empresas que coletam, armazenam e fornecem dados pessoais de variadas fontes para outras empresas. Também integram os negócios a categorização e classificação desses dados, para fins de criação de perfil e realização de publicidade direcionada. Em geral, tais empresas não integram diretamente a relação de consumo, e operam de forma totalmente desconhecida pelo titular de dados. São exemplos de empresas assim categorizadas a *Acxiom*, *Serasa Experian*, *Epsilon*, *CoreLogic*, *Datalogix*, *Intelius*, *PeekYou*, *Exactis*, *Recorded Future*, entre outras (ZANATTA, 2021, p. 958-961).

De acordo com Zanatta, muitas corretoras adotaram um discurso pró-LGPD, e justificam suas atividades não pelo consentimento, mas pelo legítimo interesse (art. 7º, XI, da LGPD). Todavia, o legítimo interesse deve ser balanceado pela legítima expectativa do titular de dados, de forma que a mera alegação não é o suficiente para justificar o tratamento.

Outro relatório mais recente, publicado em 2020, e originado de uma investigação realizada pelo Information Commissioner Office (ICO) contra as empresas Experian, Equifax e TransUnion, traz uma lição importante de que deve ser exigida uma base legal clara, bem como que os dados pessoais oferecidos devem estar em conformidade com a legislação de proteção de dados, antes de ser executado um serviço de corretagem. Segundo Elizabeth Denham, Diretora da ICO, a investigação teria revelado “falhas generalizadas e sistêmicas de proteção de dados em todo o setor”, além de “falhas significativas de proteção de dados em cada empresa” (...) para possibilitar o uso adequado de tal base legal (legítimo interesse), é necessário que seja realizado Teste de Legítimo Interesse (ou Legitimate Interests Assessment – LIA) (...) Dessa forma, a simples alegação de que a atividade de uma corretora de dados estaria

abarcada por tal base legal não seria suficiente, sendo necessária a comprovação da legitimidade da operação, por meio de apresentação da documentação dos processos realizados (ZANATTA, 2021, p. 970-972).

Conforme pontuado, para além da problemática das bases legais, a própria atividade empreendida pelos corretores de dados, sintomática do capitalismo de vigilância, gera diversas implicações quanto ao tratamento abusivo de dados, a falta de transparência e a questionável prática de “perfilização”. Para Zanatta, discute-se a possibilidade de responsabilização dessas empresas pela prática de ilícitos relacionado à atividade que, todavia, dependerá de uma interpretação extensiva da LGPD com o “Código Civil e Código de Defesa do Consumidor, e da correta interpretação dos bons precedentes já construídos pelo Superior Tribunal de Justiça no Brasil” (ZANATTA, 2021, p. 982). Por si só, a LGPD e seus critérios de bases legais não apresentam uma resposta proporcional ao risco potencialmente considerado.

Para ilustrar outras inadequações pertinentes ao modelo legislativo como um todo e seus desdobramentos, pesquisas recentes já tratam dos efeitos adversos do RGPD no mercado internacional, a exemplo do que a Google tem feito no mercado de *ad tech*. A tecnologia de publicidade (*ad tech*) é aquela destinada à elaboração de *softwares* para veicular campanhas publicitárias digitais, contratadas por anunciantes. No âmbito da tecnologia de publicidade, a Google já possui um *market share* altíssimo em todas as partes da cadeia de valor. Efetivamente, os custos de conformidade do RGPD estão esvaziando o mercado de *ad tech* e desencorajando novas iniciativas, fortalecendo a posição de todas as empresas capazes de implementá-los – as *big techs*. *Market* digital é uma área crítica para o comércio *online*, e a indústria de *ad tech* cria a ponte entre produtores de conteúdo e anunciantes (GERADIN; KARANIKIOTI; KATSIFIS, 2020, p. 47-92).

Em suma, é possível concluir que, em um contexto neoliberal de colonialismo de dados, o titular de dados brasileiro está inserido em uma complexa lógica de coleta de dados pelas *big techs*, em um regime de assimetria informacional. A legislação vigente é consequência de uma série de fatores, dentre os quais se destaca uma pronunciada motivação mercadológica e necessidade de adequação a um parâmetro internacional. Como se a lógica de exploração capitalista empreendida por empresas estadunidenses não bastasse, o titular de dados brasileiro é sujeito a um modelo internacional de legislação adequado à União Europeia, restando assim duplamente colonizado e hipervulnerável.

Ainda em relação à LGPD, as inadequações já verificadas em relação às suas bases legais e insuficiências vêm aprofundar a condição de vulnerabilidade. O Brasil é um país que não exporta tecnologia, possuindo uma economia assentada na exportação de *commodities*. É

um país com altíssimos índices de analfabetismo, evasão escolar, desemprego e a pobreza, não obstante aparelhos inteligentes sejam ubíquos mesmo entre as populações mais carentes. Assim, questiona-se se a importação de um modelo de legislação de proteção de dados europeu, que legitima uma lógica capitalizada de coleta de dados, supre as demandas da realidade social brasileira, o que naturalmente induz à necessidade de pensar alternativas presentes no ordenamento, capazes de suprir demandas sociais e coletivas.

Os fundamentos expostos não anulam o progresso representado pela LGPD, tampouco a importância de adequação do Brasil ao cenário internacional, mas sugerem que esses progressos não bastam. Há um histórico significativo de situações nas quais outras esferas do direito, além da individual, estiveram ameaçadas pela ação das *big techs*. A atribuição de responsabilidade então perpassou a aplicação de princípios fundamentais e decisões judiciais coerentes com o arcabouço jurídico brasileiro para além da LGPD, como o Marco Civil da *Internet*, o Código do Consumidor e, principalmente, a Constituição Federal.

A interpretação sistemática dessas fontes pode ajudar a delinear uma legislação brasileira sobre tecnologia da informação verdadeiramente autóctone e emancipatória. Essa legislação, embora imersa na realidade do capitalismo de vigilância, só poderia concretizar o interesse social, haja vista não ser erigida a partir de necessidades econômicas. A visão social da realidade digital capitalizada permite diversas abordagens, mister dentre elas talvez seja a noção de função social da empresa.

#### 4.2. FUNÇÃO SOCIAL DAS *BIG TECHS*: POSSIBILIDADES DE UMA LEGISLAÇÃO DE DADOS EMANCIPATÓRIA

Para Boaventura de Sousa Santos, o pensamento moderno divide a realidade social em linhas abissais, visíveis e invisíveis, de forma que as invisíveis fundamentam as visíveis. O Norte Global, “deste lado da linha”, é o centro da modernidade ocidental, e tudo que está do outro lado desaparece enquanto realidade. As imensas distinções materialmente visíveis são consequências da invisibilidade do que está do outro lado, espaço ocupado pela zona colonial (SANTOS, 2009, p. 23-26). O que acontece nas periferias, portanto, é inexistente, sequer é considerado. Nesse panorama globalizado neoliberal de colonialismo informacional, não há espaço para o consumidor do Sul global, cuja única participação é a disposição de seus dados (CASSINO, 2021, p. 30).

O pensamento abissal é capaz de impor uma dicotomia absoluta em dois domínios essenciais: o conhecimento e o direito. No que tange ao conhecimento, a crença irrestrita na

ciência determina finalisticamente o que é verdade e o que não é; no âmbito do Direito, a linha é traçada entre o legal e o ilegal. Todas as demais experiências epistemológicas e sociais são descartadas e esquecidas. Ao Sul Global, resta uma lógica de apropriação e violência (SANTOS, 2009, p. 26-30). A justificativa epistemológica é a centralidade histórica da Europa e do pensamento eurocêntrico para a modernidade. Todavia, as propostas decoloniais foram bem sucedidas em identificar que a “Europa *nunca foi o centro da história mundial* até finais do século XVIII”, passando a ser em consequência da Revolução Industrial (DUSSEL, 2009, p. 285). Como já referido anteriormente, a Revolução Industrial deve-se, em grande parte, à colonização das Américas.

Dessa forma, Boaventura de Sousa Santos propõe que o pensamento “pós-abissal” parte do reconhecimento da diversidade de experiências do mundo, que continuam desprovidas de uma epistemologia. O que foi chamado pelo autor de cosmopolitismo subalterno, veículo de um pensamento pós-abissal, teve sua semente no Fórum Social Mundial no início do século, com destaque à participação dos movimentos indígenas. O cosmopolitismo subalterno possui um *ethos* verdadeiramente redistributivo, no sentido de justiça cognitiva, material, social, política e simbólica, frente às relações de poder desiguais que ordenam o capitalismo neoliberal (SANTOS, 2009, p. 41-43). Em que pese o autor escrevesse *in media res* das mudanças relacionadas à *Internet* e às *big techs* tratadas neste trabalho, é lícito concluir, a partir de tudo que foi exposto, que a revolução tecnológica reforça o pensamento abissal.

Assim, a revolução tecnológica não configurou um caráter emancipatório, muito menos cumpriu seu potencial de valorização de *epistemes* diversas. Pelo contrário, trouxe uma nova forma de colonialidade pelas grandes empresas de tecnologia, de relações de poder que emanam do centro para a periferia, em forma de apropriação (de dados, de experiências, de mais valia) e violência (à privacidade, ao consumidor, ao mercado). As epistemologias do Sul são sobrepostas, no âmbito do conhecimento, pela lógica do capitalismo de vigilância, que limita a experiência humana com seu aspecto tecnocrático e mercadológico, e no âmbito do direito, pela europeização normativa, que subjuga possíveis soluções jurídicas locais por meio de construções estrangeiras e regras internacionais estabelecidas por países ricos.

O reconhecimento da persistência do pensamento abissal é o primeiro requisito para o pensamento pós-abissal. Considerando essa realidade juntamente com as alternativas do cosmopolitismo subalterno, Boaventura de Sousa Santos observa que a saída se encontra em uma ecologia de saberes:

Pelo contrário, o pensamento pós-abissal é um pensamento não-derivativo, envolve uma ruptura radical com as formas ocidentais modernas de pensamento e ação. No nosso tempo, pensar em termos não-derivativos significa pensar a partir da perspectiva do outro lado da linha, precisamente por o outro lado da linha ser o domínio do impensável na modernidade ocidental. A emergência do ordenamento na apropriação/violência só poderá ser enfrentada se situarmos a nossa perspectiva epistemológica na experiência social do outro lado da linha, isto é, do Sul global não-imperial, concebido como a metáfora do sofrimento humano sistêmico e injusto provocado pelo capitalismo global e pelo colonialismo (...) O pensamento pode ser sumariado como um aprender com o Sul usando uma epistemologia do Sul. Confronta a monocultura da ciência moderna com uma ecologia dos saberes. É uma ecologia, porque se baseia no reconhecimento da pluralidade de conhecimentos heterogêneos (sendo um deles a ciência moderna) e em interações sustentáveis e dinâmicas entre eles sem comprometer a sua autonomia. A ecologia de saberes baseia-se na ideia de que o conhecimento é interconhecimento (SANTOS, 2009, p. 44-45)

Define-se a ecologia de saberes como uma contra-epistemologia, que reconhece e dá validade ao pensamento pluralista. É redistribuído o valor às experiências globais não hegemônicas, como forma de resistência ao capitalismo global (SANTOS, 2009, p. 47). Nesse contexto, as soluções mais apropriadas não precisam e nem devem ser sempre as mais adequadas à realidade hegemônica do neoliberalismo, portanto, as menos custosas e mais convenientes. Sem embargo, elas devem ser compatíveis com as realidades locais e responder às demandas fundamentais de forma mais satisfatória.

O Brasil experienciou a formação do Estado social de forma tardia. Pode-se argumentar que os primeiros passos foram dados pela Constituição de 1934, fortemente inspirada pela Constituição de Weimar, de 1919, e pela Constituição Espanhola de 1931. Uma história política conturbada e diversos períodos ditatoriais justificam o advento retardatário dos direitos sociais. No entanto, a Constituição Brasileira de 1988 é referência em termos de direitos fundamentais e complexidade, e é considerada social pois regula a ordem econômica e social para além do que se pretende em um Estado liberal (SANTIAGO; CAMPELLO, 2016, p. 120). Muitas das qualidades da Constituição de 1988 decorrem de uma ênfase nas garantias, na cidadania e na democracia, como resposta a um longo período de ditadura militar, bem como de sua contemporaneidade, mais afeita às sensibilidades recentes.

Nesse sentido, a Carta Magna trouxe, em seu art. 5º, XXIII, e art. 170, III, a função social da propriedade como fundamento da ordem econômica (BRASIL, 1988). A função social da propriedade é definida pela doutrina como uma limitação ao direito fundamental de propriedade, devendo a mesma atender à sua função social. Por meio do fenômeno de constitucionalização do Direito Civil, decorre o princípio da função social dos contratos, com previsão no art. 421 do Código Civil de 2002, no sentido de que “a liberdade contratual será exercida nos limites da função social do contrato (LISBOA; VILHENA, 2020, p. 87). Dessa

forma, restou endossada a função social da empresa, partindo-se da inferência de que o contrato ou estatuto da empresa deve perseguir a função social, bem como a propriedade empresarial estará sujeita aos mesmos princípios que a propriedade comum (DINIZ, 2018, p. 394).

De forma expressa no ordenamento, a função social da empresa aparece na Lei das Sociedades Anônimas (Lei nº 6.404/76), art. 116, parágrafo único, e art. 154, *caput*, não obstante regule tipo societário específico. Sendo todos os desdobramentos da função social da propriedade e dos contratos aplicáveis à função social da empresa, esta pode ser definida como a finalidade empresarial que transcende a geração de lucros, exigindo que a atividade da empresa atenda o bem comum (LISBOA; VILHENA, 2020, p. 88).

De acordo com Maria Helena Diniz:

Pela teoria da função social empresa, o empresário e a sociedade empresária deverão ter o poder-dever de, no desenvolvimento de sua atividade, agir a serviço da coletividade. A propriedade empresarial deverá atender à função social, exigida pela Carta Magna (arts. 5º, XXII, 182, §2º, e 186); por isso o empresário exercerá sua atividade econômica organizada de produção e circulação de bens e serviços no mercado de consumo, de forma a prevalecer a livre concorrência sem que haja abuso de posição mercadológica dominante, procurando proporcionar meios para a efetiva defesa dos interesses do consumidor e a redução de desigualdades sociais, assumir funções assistenciais para seus empregados, p. ex, formando serviços médicos, fundos de previdência, planos de aposentadoria, promovendo ensino básico, creches, transporte, e, ainda, realizar projetos de recuperação do meio ambiente, e do patrimônio histórico-cultural. É preciso compatibilizar essa sua função social, visando o bem-comum, o bem-estar e a justiça social, com a finalidade de produção de lucros (DINIZ, 2018, p. 394-395).

A exploração da atividade empresarial, portanto, não interessa somente ao empresário, já que a empresa é uma convergência de fatores e interesses sociais que “devem projetar-se na vida em sociedade, atingindo empregados, fornecedores, fisco e meio ambiente” (CARDOSO; CARMO, 2017, p. 147). Dessa forma, a função social da empresa deve ser seguida no âmbito da atividade comercial buscando evitar abusos econômicos, em termos de gestão procurando suprir exigências do bem comum e prestação de contas, nas relações com o consumidor para atender seus direitos básicos e na relação com o meio ambiente, buscando sua preservação e em consonância com os demais princípios da ordem econômica (DINIZ, 2018, p. 397-408).

Em termos globais, a responsabilidade social da empresa é uma questão antiga. Desde o final do século XIX, empresas em grandes centros econômicos começaram a desenvolver uma abordagem paternalista em relação a seus empregados, clientes e comunidade. Após a Segunda Guerra Mundial, discussões sobre responsabilidades concretas das empresas para com as pessoas tornaram-se mais prementes. Já na metade do século XX, autores como Howard Bowen identificavam o impacto tangível das empresas na sociedade, de forma que os empresários

deveriam levar em consideração os impactos sociais de suas decisões. A despeito do conturbado movimento político dos anos 1970, as discussões sobre *Corporate Social Responsibility* (CSR) ficaram limitadas às ações discricionárias que as empresas poderiam tomar em relação ao meio ambiente e aos trabalhadores. A definição exata de CSR restava ainda incompleta (AGUDELO; DAVÍDSDÓTTIR, 2019, p. 3-15).

As décadas de 1990 e 2000 serviram para consolidar as noções de CSR, incluindo uma nova expressão ao termo: *strategic* (estratégica). De acordo com Agudelo e Davídsdóttir:

A forma como Lantos (2001) explicou os limites de CSR foi provavelmente a primeira vez que o termo *estratégica* foi ligada à CSR. Desde então, a literatura começou a incluir aspectos *estratégicos* no conceito (...) Porter e Kramer (2006) construíram sobre a noção de que empresas podem alcançar vantagens competitivas através da SCSR e explicaram que empresas podem abordar seus contextos competitivos por meio de um estratégia que resulta na criação de valor compartilhado na forma de benefícios para a sociedade enquanto melhoram a competitividade da empresa. Para Porter e Kramer, a empresa primeiro deve olhar de dentro para fora para mapear o impacto social de sua cadeia de valores e identificar os efeitos positivos e negativos de suas atividades na sociedade e então focar naqueles com o maior valor estratégico (...) Ao final dos anos 2000, SCSR era compreendida como tendo potencial para gerar valor compartilhado e abordar preocupações sociais (AGUDELO; DAVÍDSDÓTTIR, 2019, p. 12). [tradução nossa].

Portanto, as décadas de 2000 e 2010 serviram para reforçar uma noção de responsabilidade corporativa *estratégica*, na qual a empresa é motivada a abordar aqueles problemas sociais que impedem a maximização do lucro. Assim, é evidente o contexto no qual o capitalismo de plataforma se desenvolve, na lógica neoliberal do que Morozov chamou de solucionismo (MOROZOV, 2018, p. 16). O Estado, atrofiado e a serviço das empresas, repassa atribuições à iniciativa privada que, por sua vez, internaliza aquelas que lhe são economicamente convenientes. O aspecto estratégico da SCSR (responsabilidade corporativa estratégica) faz dela uma construção essencialmente nortista e mercadológica.

Em comparação com a função social da empresa, os contrastes são evidentes. A função é a capacidade e dever de dar destino ao objeto. Para a função social, o alinhamento da empresa com os interesses comunitários é de tal forma pronunciado que uma destinação conflitante com o bem comum acarretará o descumprimento desta função. A empresa jamais poderá se valer de suas atividades para justificar lesão à coletividade. Em outras palavras, da mesma forma que a função social da propriedade limita o direito à propriedade, a função social da empresa limita a livre iniciativa (CARDOSO; CARMO, 2017, p. 148).

Dessa forma, a função social faz parte de uma ecologia de saberes do Sul, própria da experiência brasileira e de toda a construção jurídica, jurisprudencial e doutrinária nacional.



Nesse sentido, pode ser vista como instrumento apto para atender as demandas locais em face das soluções importadas de países desenvolvidos, bem como das novas lógicas de colonialidade. Representaria, portanto, uma alternativa de pensamento pós-abissal para um arcabouço jurídico emancipatório em relação à tecnologia. Na sequência, serão trazidas algumas possibilidades da aplicação e perspectivas do titular de dados brasileiro, sem a pretensão de esgotar o tema, objetivando-se explorar as implicações mais imediatas e pertinentes da proposta, ensejando novos desenvolvimentos futuros do tema.

Resta a questão da possibilidade da aplicação da função social às *big techs*. Frequentemente, o cumprimento da função social da empresa no âmbito das empresas de tecnologia está vinculado ao *compliance* com a LGPD (PUJOL; RYNDACK, 2021, p. 197). Todavia, como já tratado anteriormente, a LGPD possui limitações sintomáticas de sua natureza mercadológica e derivativa. No passado, a atribuição de responsabilidade das *big techs* então perpassou a aplicação de princípios fundamentais e decisões judiciais coerentes com o arcabouço jurídico brasileiro para além da LGPD, como o Marco Civil da *Internet*, o Código do Consumidor e a Constituição Federal. A interpretação sistemática dessas fontes pode ajudar a delinear uma legislação brasileira sobre tecnologia da informação verdadeiramente emancipatória e coerente com a função social da empresa.

Justificadamente, convencionou-se categorizar o empreendedorismo tecnológico de inovação de empresas como as *startups* como um empreendedorismo de alto impacto. Essa nova forma de empreendedorismo pode ser definida da seguinte forma:

Ao inserir o artigo 65-A na Lei Complementar nº 123, de 14 de dezembro de 2006 (Lei do Simples Nacional), a Lei Complementar nº 167 de 24 de abril de 2019 tentou conceituar startups definindo suas características e diferenciando as startups de natureza incremental das startups de caráter disruptivo. Do referido dispositivo pode-se extrair que, para o ordenamento jurídico brasileiro, as startups são: agentes indutores de avanços tecnológicos e de geração de emprego e renda, caracterizadas pelo desenvolvimento de inovações, em condições de incerteza e que requerem experimentos e validações, que podem produzir sistemas, métodos ou modelos de negócio, serviços ou produtos totalmente novos (startups de natureza disruptiva) ou aperfeiçoar os já existentes (startups de natureza incremental) (...) O empreendedorismo de alto impacto, seja disruptivo ou incremental, produz alterações no mercado econômico e na sociedade, se diferenciando do empreendedorismo de subsistência ou caseiro, de alcance mais restrito e normalmente ligado a necessidade de complementação ou manutenção da renda familiar. Tais empresas inovadoras apresentam crescimento disruptivo, causam grande impacto no mercado econômico (...) (PUJOL; RYNDACK, 2021, p. 190-191).

Indubitavelmente, a necessidade de *compliance* com a legislação nacional se aplica às *startups* e às empresas de tecnologia que atuam no território nacional. Como referido, a atuação da empresa deve estar de acordo não somente com a LGPD, mas também com o restante do

ordenamento nacional. Em que pese remanesça a dificuldade de se exigir que empresas multinacionais tenham afinidade com os interesses nacionais, tal fato não pode justificar a inobservância das disposições do ordenamento pátrio, sendo inadmissível que a contratação para atuar em território nacional seja um ato de concessões unilaterais (SANTIAGO; CAMPELLO, 2016, p. 133).

Referir que a atuação das *big techs* é empreendedorismo de alto impacto seria um eufemismo. As *big techs*, na condição de atores globais, pelas razões expostas no primeiro capítulo deste trabalho, ditam a lógica da vida moderna. Tais empresas não invadiram apenas o rol de companhias mais lucrativas do mundo, mas foram capazes de instituir uma nova realidade neoliberal tecnocrática, de vigilância, exploração e coleta de dados. As tecnologias e sistemas capitaneados por esses empreendimentos tornaram-se condição de existência para o comércio contemporâneo e para a prestação de serviços, inclusive públicos. O poder das grandes empresas de tecnologia não possui paralelo na história da humanidade.

A despeito desse poder, grandes empresas de tecnologia ainda gozam dos benefícios das *startups*, justificados pelo risco do empreendimento e pela promessa de lucro. As *big techs* estão isentas da necessidade de respeitar a integridade do mercado de capitais ou a completa transparência para com o usuário, pois o descumprimento dessas regras não lhes acarretará consequências significativas. Além disso, pela própria lógica de funcionamento e concentração decisória dessas empresas, a atuação das *big techs* não gera empregos locais. Cada vez mais, as funções básicas e serviços são automatizados para maximizar a acumulação de lucros e, em que pese devessem possuir sede no Brasil, muitas empresas de tecnologia não o fazem ou o fizeram de forma retardatária, sem que essas sedes representem alguma participação significativa no funcionamento da empresa. A exteriorização dos lucros é a regra.

Assim, essas empresas atuam majoritariamente sem a contraprestação social do lucro que obtêm a partir do tratamento de dados do titular brasileiro. Uma primeira consequência do respeito à função social da empresa viria na forma de abstenção. Para além do respeito às regras do mercado nacional, tais empresas não podem atuar de forma a obstar a criação de soluções locais para problemas locais. Exemplo emblemático é trazido por Sérgio Amadeu, que narra a negociação do Poder Judiciário de São Paulo com a Microsoft em 2019. Segundo o noticiário especializado, o TJSP iria negociar, com dispensa de licitação, a criação de uma Plataforma de Justiça Digital de armazenamento de processos na nuvem com a empresa estadunidense. Milhões de dados sensíveis de processos, pessoas e empresas brasileiras quase foram entregues a uma plataforma estrangeira, com interesses econômicos e geopolíticos no Brasil (SILVEIRA, 2021, p. 33-36).

A operação descrita acima não se concretizou por decisão do CNJ, porém essa já é a realidade de outros órgãos nacionais. Em 2020, o Ministério da Educação negociou pela entrega dos dados do SiSU (Sistema de Seleção Unificada) à plataforma na nuvem da Microsoft chamada Azure. Lá estão armazenados os dados de desempenho escolar de milhões de estudantes brasileiros (SILVEIRA, 2021, p. 40). A justificativa, em ambos os casos, é a redução do custo com *data centers* locais. A consequência acaba sendo a atrofia da tecnologia nacional e a livre disposição de dados sensíveis às empresas estrangeiras. Esse dano ao bem comum a longo prazo evidentemente não influi na conta do Poder Público, o que garante vantagem às grandes empresas de tecnologia.

Um segundo aspecto do respeito à função social exsurge em relação à capacidade de acesso a essas empresas. O caso Telegram é emblemático para estabelecer a importância da empresa possuir sede no Brasil. Em 2021, não foi atendida ordem de bloqueio e sanção ao canal do blogueiro Allan dos Santos exarada pelo STF, em escândalo relacionado à disseminação de *fake news*. Inicialmente, o Telegram, sem sede no Brasil, ignorou todas as tentativas de contato do Ministério Público Federal e do Tribunal Superior Eleitoral. Apenas na iminência de ser bloqueado em todo o território nacional por determinação do Ministro Alexandre de Moraes, do STF, o aplicativo respondeu e obedeceu à ordem judicial (MARTINS, MEDEIROS, PESSOA, 2022, p. 12).

A necessidade das grandes empresas de tecnologia possuírem sede no Brasil pode ser interpretada no ordenamento na forma do art. 6º, VI, do CDC, quando dispõe que “a efetiva prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos” (CDC, 1990). Apesar dos contratos com as *big techs* contarem com cláusula de eleição de foro, dispõe o CDC, em seu art. 101, I, que a ação de responsabilidade civil manejada contra o fornecedor poderá ser proposta no domicílio do autor. Evidentemente, o consumidor dificilmente estará suficientemente atendido em suas demandas enquanto o acesso à empresa lhe for obstado ou dificultoso. O Marco Civil da *Internet*, em seu art. 11, § 2º, reforça que deve ser respeitada a legislação nacional em qualquer operação de coleta, tratamento ou registro de dados “mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que ofereça serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil” (MCI, 2014).

Por fim, o reconhecimento da exploração de um *superávit* comportamental advém logicamente da ausência de uma compensação ao titular. Particularmente em países periféricos, o tratamento de dados pode ter efeitos nefastos para a coletividade. Para cibercriminosos, os dados dos brasileiros estão entre os mais baratos do mundo, sintomas da baixa segurança e da

assimetria informacional. De acordo com dados da *NordVPN*, o país ocupa a 15ª posição entre os países com maior quantidade de informações financeiras vazadas, e 8ª posição dos menores preços cobrados por criminosos<sup>3</sup>. Em termos puramente mercadológicos, o titular de dados brasileiro possui menos valor para “negociar” do que qualquer titular de um país rico, bem como menos segurança e meios de acesso e resposta. Seus dados sequer são tratados em seu território, e as contraprestações pelo tratamento (melhoria dos serviços), quando existem, chegam mais precariamente à colônia.

Algumas discussões já foram levantadas sobre a cobrança pelo tratamento de dados. Em termos de função social da empresa, a atuação das grandes empresas de tecnologia não retorna à sociedade de forma satisfatória para “criação de novos empregos e formação de mão de obra qualificada; salário do trabalhador, permitindo sua sobrevivência e a de sua família; tributos, possibilitando a consecução das finalidades do poder público e a manutenção do Estado” (DINIZ, 2018, p. 396). Sobra apenas uma exploração condicionada e desavisada, com enormes benefícios para as empresas. A compensação por essa exploração possui diversos suportes, seja uma melhor adequação à função social, seja a compreensão do direito dos titulares como um direito difuso e coletivo (como na esfera ambiental), cuja exploração dos dados com potencial danoso (recursos) deveria ser ressarcida pelas empresas na condição de explorador-pagador (poluidor pagador).

Na linha do pensamento pós-abissal, emancipatório e garantidor da função social da empresa, a instituição de uma taxa módica da exploração de dados, coletada pela Administração Pública, teria destinação não para compensação particular do titular, mas para a arrecadação de fundos de financiamento para a tecnologia local. Também não se exclui a possibilidade do financiamento de políticas de capacitação informacional para a coletividade, de forma a empoderar o titular de dados em relação a todos os aspectos da exploração para, só assim, requalificar o consentimento como alternativa válida e consciente diante da assimetria material e informacional.

Assim, a utilização da função social da empresa aplicada às *big techs* constitui uma alternativa jurídica do Sul global à colonialidade e ao pensamento abissal. A partir da pesquisa realizada, três possibilidades interpretativas emergem a partir do ordenamento, extrapolando os limites da Lei Geral de Proteção de Dados Pessoais. Inicialmente, essas empresas deveriam estar impedidas de interferir na infraestrutura do Estado e obstar a criação de soluções

---

<sup>3</sup> CANALTECH. **Dados pessoais de brasileiros estão entre os mais baratos do mundo no cibercrime**. 2022. Disponível em <https://canaltech.com.br/seguranca/dados-pessoais-de-brasileiros-estao-entre-os-mais-baratos-do-mundo-no-cibercrime-218546/>. Acesso em: 16 nov. 2023.

tecnológicas locais. Da mesma forma, os dados de brasileiros deveriam ser tratados no Brasil, e as empresas não poderiam se escusar de possuir sede no país. Por fim, a cobrança de uma taxa módica em contrapartida à exploração dos dados, revertida para finalidade coletivas.

## 5. CONCLUSÃO

A pesquisa realizada buscou explorar as perspectivas do titular de dados brasileiro frente ao capitalismo de vigilância e a europeização normativa, duas manifestações de um colonialismo próprio da contemporaneidade. Para tanto, propôs-se ponderar as possíveis soluções jurídicas autóctones, a partir da função social da empresa aplicada às *big techs*, identificando-se em que medida as lógicas vigentes são problemáticas do ponto de vista social e regulatório e quais alternativas podem ser extraídas da experiência brasileira.

De início, partiu-se da visão de Manuel Castells sobre a nova economia, na esteira dos primórdios da *internet* e do advento das novas tecnologias informacionais, para evidenciar o contraste com as críticas das teorias contemporâneas, como a trazida por Shoshana Zuboff ao conceituar o capitalismo de vigilância. Em virtude das ascensão das *big techs*, constatou-se que o deslumbramento com a tecnologia culminou na despolitização do debate e na normalização de uma realidade neoliberal de exploração de dados excessiva, na qual o titular possui pouco ou nenhum conhecimento sobre o processo de tratamento de dados.

Posteriormente, analisou-se a história do direito à privacidade e à proteção dos dados pessoais em suas diversas manifestações regulatórias, internacionais e nacionais. Foram tratadas as divergências doutrinárias sobre o próprio conceito de privacidade e as dificuldades de regulação efetiva desse direito. Resta claro que, malgrado tais discussões não sejam recentes, estiveram sempre ligadas ao desenvolvimento de novas tecnologias e formas de exploração de dados, tendo origem em países europeus que entabularam uma verdadeira tradição regulatória, a qual viria a se difundir internacionalmente, em especial após o Regulamento Geral sobre a Proteção de Dados.

Consequentemente, fez-se necessária a exploração desse fenômeno de difusão normativa através da teoria do Efeito Bruxelas, de Anu Bradford. Constatou-se a capacidade da União Europeia de impor regras a determinados mercados. Apontaram-se casos de manifestação de ambos os aspectos do Efeito Bruxelas, *de jure* e *de facto*, ocorrendo internacionalmente a partir da influência legislativa europeia. Também se observou a assunção do papel de regulador mundial de fato no âmbito da proteção de dados pela União Europeia, oferecendo um contraponto à abordagem regulatória estadunidense.

Assim sendo, a comparação entre o Regulamento Geral sobre a Proteção de Dados europeu e a Lei Geral de Proteção de Dados Pessoais brasileira comprovou a ocorrência do fenômeno de europeização normativa. Em seu aspecto *de facto*, à vista do intenso *lobby* praticado pelo setor privado ao longo do processo legislativo da lei brasileira; em seu aspecto

*de jure*, na clara transposição de princípios, bases legais e artigos da norma europeia. Ainda que não inicialmente prejudicial, o reconhecimento dessa influência justificou o receio acerca das motivações do modelo legal, haja vista a incorporação de normas estar carregada de interesses do local de origem.

Dessa forma, constatou-se a ocorrência de uma colonialidade dúplice, tanto na forma das tecnologias como das leis. A lei de proteção de dados está eivada de interesses e influências externas, alheias à realidade brasileira, configurando uma lógica que favorece as *big techs*. Inicialmente, foram explorados os descompassos da legislação de dados vigente (LGPD) com a realidade de um país emergente, sobre o aspecto de uma nova colonialidade de dados explicada por Sérgio Amadeu, que encontra solo fértil em uma economia neoliberal e nas motivações mercadológicas do modelo legislativo, institucionalizante da mercantilização de dados.

Por fim, foram exploradas alternativas jurídicas para um pensamento pós-abissal, emancipatório e originário do Sul global. A partir da experiência e do ordenamento nacional, surge a função social da empresa, diversa do conceito de *Corporate Social Responsibility*, que baliza a ordem econômica constitucional para fins de concretizar o Estado social. A função social da empresa foi interpretada aqui como uma compreensão holística do conjunto de legislações brasileiras sobre tecnologia, dados, segurança e consumerista, para fins de efetivar garantias e direitos fundamentais dos titulares frente às *big techs*.

Certo é que a discussão não foi esgotada. O presente trabalho buscou meramente identificar caminhos possíveis diante da realidade apresentada. Como leciona Boaventura de Sousa Santos, o passo primordial é a compreensão do pensamento abissal e da condição de colonialidade. Nesse aspecto, não se objetiva desqualificar os avanços e as conveniências da vida moderna trazidas pela tecnologia, tampouco o embaraço da pesquisa para novas soluções e futuros empreendimentos. Doutra banda, esta pesquisa vai ao encontro de uma tradição sociológica e teórica de pesquisadores, consolidada na última década, que observa com apreensão o salvo conduto dado às grandes empresas de tecnologia para atuarem como bem entendem, a vulnerabilidade do usuário e titular de dados e a despolitização do debate acerca da tecnologia.

Da mesma forma, não se trata de vilanizar a adesão a modelos legislativos e convenções estrangeiras. É de grande importância que exista harmonia entre o Brasil e os demais membros da comunidade internacional. Dito isto, a pesquisa buscou evidenciar a postura acrítica e mercadológica frente ao fenômeno de europeização normativa, sintomático de uma globalização neoliberal e homogeneizadora. É de suma importância que essas condições sejam

reconhecidas e discutidas no âmbito da academia, haja vista se tratar de realidade ubíqua e em constante recrudescimento.

Em que pese o direito esteja em permanente atraso em face das novas realidades sociais, não é lícito ficar inerte diante de um contexto que favorece reiteradas violações. Para além das discussões técnicas e econômicas, o direito precisa estar inserido em sua dimensão cultural, como reflexo de uma experiência humana no Sul global. O ordenamento jurídico brasileiro é lar de significativas vanguardas normativas e jurisprudenciais em termos de direitos fundamentais, nascidas de uma complexa e rica realidade social, com ênfase na Constituição Federal. A alternativa trazida é apenas um esboço para a construção de propostas normativas adequadas à realidade brasileira.



## REFERÊNCIAS

ABREU, Karen Cristina Kraemer. História e Usos da Internet. BOCC. **Biblioteca On-line de Ciências da Comunicação**, v. 2009, p. 01-09, 2009. ISSN: 1646-3137. Disponível em <https://www.bocc.ubi.pt/pag/abreu-karen-historia-e-usos-da-internet.pdf>. Acesso em: 02 out. 2023.

AGUDELO, Mauricio Andrés Latapí; JÓHANNSDÓTTIR, Lára; DAVÍDSDÓTTIR, Brynhildur. A literature review of the history and evolution of corporate social responsibility. **International Journal of Corporate Social Responsibility**, 4:1, 2019, DOI: <https://doi.org/10.1186/s40991-018-0039-y>. Disponível em <https://jcsr.springeropen.com/articles/10.1186/s40991-018-0039-y?uc=racialjustice>. Acesso em: 02 out. 2023.

APPLE. **Apple Privacy Policy**. Cupertino, CA: APPLE, 2022. Disponível em <https://www.apple.com/legal/privacy/en-ww/>. Acesso em: 02 out. 2023.

BIONI, Bruno *et al.* **Proteção de dados: contexto, narrativas e elementos fundantes**. 1. ed. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BRADFORD, Anu. The Brussels Effect. Bradford, **Northwestern University Law Review**, vol. 107, n. 1, 2012. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2770634](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634). Acesso em: 02 out. 2023.

BRASSCOM. **Manifesto pela aprovação da Lei de Proteção de Dados Pessoais**. Brasília: BRASSCOM, 2018. Disponível em: <https://brasscom.org.br/pdfs/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/>. Acesso em: 16 nov. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília: Presidência da República, [2016]. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 16 nov. 2023.

BRASIL. **Lei nº 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília: Presidência da República, 1990. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/18078compilado.htm](https://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm). Acesso em: 16 nov. 2023.

BRASIL. **Lei Complementar nº 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília: Presidência da República, 2002. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/2002/110406compilada.htm](https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm). Acesso em: 16 nov. 2023.

BRASIL. **Lei nº 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: Presidência da República, 2014. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 16 nov. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 4060/2012**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Brasília: Câmara dos

Deputados, 2012. Disponível em: <https://www.congressonacional.leg.br/materias/materias-bicameras/-/ver/pl-4060-2012>. Acesso em: 02 out. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais - (LGPD). Brasília: Presidência da República, 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 16 nov. 2023.

BORNELI, Junior. Apple, Google e mais: quantos milhões as big techs ganham por hora. **Startse**, 2023. Disponível em: <https://www.startse.com/artigos/volume-de-receita-por-horas-das-big-techs/>

CANCELIER, Mikhail Vieira de Lorenzi. **Infinito particular: privacidade no século XXI e a manutenção do direito de estar só**. 2016. Tese (Doutorado em Direito) - Centro de Ciências Jurídicas, Universidade Federal de Santa Catarina, Florianópolis, 2016. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/174424>. Acesso em: 16 nov. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. Direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Seqüência (Florianópolis)**, n. 76, p. 213-240, ago. 2017. DOI: <https://doi.org/10.5007/2177-7055.2017v38n76p213>. Disponível em <https://www.scielo.br/j/seq/a/ZNmGSYVR8kfvZGYWW7g6nJD/>. Acesso em: 16 nov. 2023.

CARDOSO, Gleissa Mendonça Faria; CARMO, Valter Moura do. Função social/solidária da empresa nos negócios virtuais. **R. Jur. UNI7**, Fortaleza, v. 14, n. 2, p. 137-157, jul./dez. 2017. Disponível em <https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/509#:~:text=A%20fun%C3%A7%C3%A3o%20social%2Fsolid%C3%A1ria%20visa,para%20presentes%20e%20futuras%20gera%C3%A7%C3%B5es>. Acesso em : 16 nov. 2023.

CASSINO, João Francisco. O sul global e os desafios pós-coloniais na era digital. *In*: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. 1.ed. São Paulo: Autonomia literária, 2021. p. 13-32.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. 1.ed. Rio de Janeiro: Zahar, 2003.

COOLEY, Thomas. **A treatise on the Law of Torts or the Wrongs which Arise Independent of Contract**. Chicago: Callaghan and Company, 1879. Disponível em: <https://repository.law.umich.edu/books/11/>. Acesso em : 16 nov. 2023.

DEMARTINI, Felipe. Dados pessoais de brasileiros estão entre os mais baratos do mundo no cibercrime. **Canaltech**, 2022. Disponível em <https://canaltech.com.br/seguranca/dados-pessoais-de-brasileiros-estao-entre-os-mais-baratos-do-mundo-no-cibercrime-218546/>. Acesso em : 16 nov. 2023.

DINIZ, Maria Helena. A importância da função social da empresa. **Revista Jurídica UNICURITIBA**, Curitiba, v. 02, n. 51, p. 387-412, 2018. Disponível em

<https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2815>. Acesso em : 16 nov. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: RT, 2019.

DUSSEL, Enrique. Meditações anti-cartesianas sobre a origem do anti-discurso filosófico da modernidade. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul**. 1. ed. Coimbra: Edições Almedina, 2009. p. 283-336.

EMPOLI, Giuliano Da. **Os engenheiros do caos**. 1. ed. São Paulo: Vestígio, 2019.

FACHIN, Zulmar. O RGPD e a LGPD: diálogos reais no mundo virtual e a proteção de direitos da personalidade. **Revista Jurídica Luso-Brasileira**, Lisboa, Ano 8, n. 5, p. 1549-1569, 2022. Disponível em <https://www.cidp.pt/publicacao/revista-juridica-lusobrasileira-ano-8-2022-n-5/280>. Acesso em: 16 nov. 2023.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Privacidade e proteção de dados pessoais: perspectiva histórica. **InCID: Revista de Ciência da Informação e Documentação**, v. 12, n. 2, p. 151-172, 2021. DOI: 10.11606/issn.2178-2075.v12i2p151-172. Disponível em: <https://www.revistas.usp.br/incid/article/view/179778>. Acesso em: 16 nov. 2023.

[FIB11] Transferência internacional e o sistema de proteção de dados pessoais no Brasil. 1 vídeo (1h 37 min). Workshop publicado pelo canal NICBrvídeos. Disponível em [https://www.youtube.com/watch?v=NW\\_zyk8-f5Y&ab\\_channel=NICBrvideos](https://www.youtube.com/watch?v=NW_zyk8-f5Y&ab_channel=NICBrvideos). Acesso em: 16 nov. 2023.

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**, Rio de Janeiro, vol. 12, n. 2, , p. 1002-1033, 2021. DOI: 10.1590/2179-8966/2020/46944. Disponível em <https://www.scielo.br/j/rdp/a/hTqmGJVy7FP5PWq4Z7RsbCG/?lang=pt>. Acesso em: 16 nov. 2023.

FOROOHAR, Rana. **Don't be evil: how big tech betrayed its founding principles - and all of us**. 1. ed. Nova Iorque: Currency, 2019.

GERADIN, Damien; KARANIKIOTI, Theano; KATSIFIS, Dimitrios. GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech. **European Competition Journal**, 17:1, p. 47-92. DOI: 10.1080/17441056.2020.1848059. Disponível em <https://www.tandfonline.com/doi/full/10.1080/17441056.2020.1848059>. Acesso em: 16 nov. 2023.

GUNST, Simon; VILLE, Ferdi de. The Brussels effect: how the GDPR Conquered Silicon Valley. **European Foreign Affairs Review**, v. 26, n. 3, p. 437– 458, 2021. Disponível em: <https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036>. Acesso em: 16 nov. 2023.

HAN, BYUNG-CHUL. **Infocracia: digitalização e a crise da democracia**. 1. ed. Rio de Janeiro: Vozes, 2022.

KIRA, Beatriz; COUTINHO, Diogo R.; GONÇALVES, Priscila Brolio. As big techs e a nova onda de regulação digital: o caso da União Europeia. **Jota**, 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/as-big-techs-e-a-nova-onda-de-regulacao-digital-o-caso-uniao-europeia-21072022>. Acesso em: 16 nov. 2023.

LIMBERGER, Têmis. Da evolução do direito de ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos**, Itajaí, v. 14, n. 2, p. 27-53, 2009. Acesso em: 16 nov. 2023.

LISBOA, Anna Luiza de Carvalho; VILHENA, Marília Marques Rêgo. Proteção de dados: nova dimensão da função social da empresa. **Revista Governança e Direitos Fundamentais**, Porto, v. 1, n. 1, p. 83-92, 2020. Disponível em <https://dialnet.unirioja.es/servlet/articulo?codigo=7474779>. Acesso em: 16 nov. 2023.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. **Revista de Direito**, Viçosa, v. 12, n. 2, p. 1-33, 2020. Disponível em <https://periodicos.ufv.br/revistadir/article/view/10597>. Acesso em: 16 nov. 2023.

MARTINS, Cássio Sbicigo; PESSOA, João Pedro Seefeldt; MEDEIROS, Arthur Zamurano. Uma leitura sócio-política do tecnopopulismo no Brasil em 2022. *In*: BASTOS, Bruna; BERNST, Luísa Giuliani. **Direito e política no Brasil contemporâneo: reflexões interdisciplinares**. 1. ed. Cruz Alta: Ilustração, 2023.

MOROZOV, Evgeny. **Big Tech**. 1. ed. São Paulo: Ubu Editora, 2018.

MUCHIUTI, Marília Machado. **Do RGPD à LGPD: difusão internacional de normas e o caso das regulamentações de proteção de dados pessoais**. 2022. Tese (Mestrado Profissional em Governança e Formulação de Políticas Internacionais) - Pontifícia Universidade Católica de São Paulo (PUC-SP), 2022.

TURNER, David; MUÑOZ, Jesus. **Para os filhos dos filhos de nossos filhos: uma visão da sociedade internet**. 1. ed. São Paulo: Summus, 2002.

PESSOA, João Pedro Seefeldt. **Cibersegurança na era dos dados e humanismo digital: a construção de um direito**. 2023. Tese (Projeto de Qualificação de Doutorado) - Universidade do Vale do Rio dos Sinos (UNISINOS), 2023.

PUJOL, Luiz Fernando Obladen; RYNDACK, Jaqueline Maria. Empreendedorismo disruptivo e ética: a importância do *compliance* e da interiorização da função social da empresa pelas *startups*. **Revista Diálogos Possíveis**, Salvador, v. 20, n. 2, p. 187-202, 2021. Disponível em <https://revista.grupofaveni.com.br/index.php/dialogospossiveis/article/view/625>. Acesso em: 16 nov. 2023.

ROUSSEAU, Jean Jacques. **O Contrato Social**. 1. ed. Oeiras: Editorial Presença, 2010.

RUARO, R. L. Algumas reflexões em torno do RGPD, em especial quanto ao consentimento, com alusões à LGPD: Um exercício interpretativo. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 14, n. 42, p. 219–249, 2020. DOI: 10.30899/dfj.v14i42.760. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/760>. Acesso em: 16 nov. 2023.

RYNGAERT, Cedric; TAYLOR, Mistale. The GDPR as global data protection regulation? **Symposium on the GDPR and international law**, AJIL Unbound, n. 114, p. 5-9. DOI:10.1017/aju.2019.80. Disponível: <https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688>. Acesso em: 16 nov. 2023.

SANTIAGO, Mariana Ribeiro; CAMPELLO, Livia Gaigher Bósio. Função social e solidária da empresa na dinâmica da sociedade de consumo. **SCIENTIA IURIS**, Londrina, v.20, n.1, p.119-143, abr. 2016. DOI: 10.5433/2178-8189.2016v20n1p119. Disponível em <https://www.e-publicacoes.uerj.br/index.php/rfduerj/article/view/18248>. Acesso em: 16 nov. 2023.

SANTOS, Boaventura de Sousa. Para além do pensamento abissal: das linhas globais a uma ecologia dos saberes. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul**. 1. ed. Coimbra: Edições Almedina, 2009. p. 23-72.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. **Revista Privacidade e Proteção de Dados**, v. 1, n. 1, p. 1-49, 2021. Disponível em <https://repositorio.pucrs.br/dspace/handle/10923/18868>. Acesso em: 16 nov. 2023.

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. *In*: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. 1.ed. São Paulo: Autonomia literária, 2021. p. 33-52.

SRNICEK, Nick. **Platform Capitalism**. 1. ed. Cambridge: Polity Press, 2016.

UNIÃO EUROPEIA. **Parlamento Europeu**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no 69 que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 16 nov. 2023.

VAIDHYANATHAN, Siva. **A Googlelização de tudo**. 1. ed. São Paulo: Cultrix, 2011.

VIANNA, Fernando Ressetti Pinheiro Marques. Se os dados são o novo petróleo, onde estão os royalties? O neoliberalismo na era dos dados. **Revista Gestão e Conexões**, Vitória, v. 10, n. 3, p. 123-143. Disponível em <https://periodicos.ufes.br/ppgadm/article/view/36014>. Acesso em: 16 nov. 2023.

ZANATTA, Rafael; SECAF, Helena; MENDONÇA, Julia. A aplicabilidade da Lei Geral de Proteção de Dados Pessoais aos corretores de dados. *In*: VILLAS BOAS CUEVA, Ricardo;

FRAZÃO, Ana. **Compliance e Políticas de Proteção de Dados**. 1. ed. São Paulo: Thomson Reuters, 2021, p. 957-988.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. *Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação*. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (org.). **Tecnopolíticas da Vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018, p. 17-68.

NUP: 23081.154952/2023-90

Prioridade: Normal

Homologação de ata de defesa de TCC e estágio de graduação

125.322 - Bancas examinadoras de TCC: indicação e atuação

### COMPONENTE

Ordem	Descrição
7	TCC

Nome do arquivo

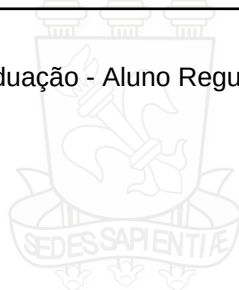
Monografia - Cássio Sbicigo Martins.pdf

### Assinaturas

09/12/2023 13:01:21

CÁSSIO SBICIGO MARTINS (Aluno de Graduação - Aluno Regular)

06.09.05.01.0.0 - Direito Diurno - 13850



1960



1960

Código Verificador: 3622203

Código CRC: f597253a

Consulte em: <https://portal.ufsm.br/documentos/publico/autenticacao/assinaturas.html>

