



UNIVERSIDADE FEDERAL DE SANTA CATARINA  
CENTRO DE CIÊNCIAS JURÍDICAS  
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Gustavo Xavier de Camargo

**A VEDAÇÃO À GRATUIDADE COMPULSÓRIA DOS SERVIÇOS DIGITAIS COMO  
FORMA DE PROTEÇÃO DOS DADOS PESSOAIS DOS USUÁRIOS  
CONSUMIDORES E MITIGAÇÃO DO ABUSO DE POSIÇÃO DOMINANTE PELAS  
PLATAFORMAS DE DOIS OU MÚLTIPLOS LADOS**

Florianópolis, SC  
2020

Gustavo Xavier de Camargo

**A VEDAÇÃO À GRATUIDADE COMPULSÓRIA DOS SERVIÇOS DIGITAIS COMO  
FORMA DE PROTEÇÃO DOS DADOS PESSOAIS DOS USUÁRIOS  
CONSUMIDORES E MITIGAÇÃO DO ABUSO DE POSIÇÃO DOMINANTE PELAS  
PLATAFORMAS DE DOIS OU MÚLTIPLOS LADOS**

Dissertação submetida ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina para a obtenção do título de mestre em Direito, área de concentração Direito, Estado e Sociedade.

Orientadora: Carolina Medeiros Bahia, Dra.

Florianópolis, SC

2020

Ficha de identificação da obra elaborada pelo autor,  
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Camargo, Gustavo Xavier de

A vedação à gratuidade compulsória dos serviços digitais como forma de proteção dos dados pessoais dos usuários consumidores e mitigação do abuso de posição dominante pelas plataformas de dois ou múltiplos lados / Gustavo Xavier de Camargo ; orientadora, Carolina Medeiros Bahia, 2020.

213 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós Graduação em Direito, Florianópolis, 2020.

Inclui referências.

1. Direito. 2. Proteção de dados pessoais. 3. Plataformas de dois lados. 4. Regulação. I. Bahia, Carolina Medeiros. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. III. Título.

Gustavo Xavier de Camargo

**A VEDAÇÃO À GRATUIDADE COMPULSÓRIA DOS SERVIÇOS DIGITAIS COMO  
FORMA DE PROTEÇÃO DOS DADOS PESSOAIS DOS USUÁRIOS  
CONSUMIDORES E MITIGAÇÃO DO ABUSO DE POSIÇÃO DOMINANTE PELAS  
PLATAFORMAS DE DOIS OU MÚLTIPLOS LADOS**

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca  
examinadora composta pelos seguintes membros:

Prof.(a) Carolina Medeiros Bahia, Dr(a).  
Universidade Federal de Santa Catarina

Prof.(a) Liz Beatriz Sass, Dr(a).  
Universidade Federal de Santa Catarina

Prof.(a) Reginaldo Pereira, Dr(a).  
Universidade Comunitária da Região de Chapecó - Unochapecó

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi  
julgado adequado para obtenção do título de mestre em Direito, área de concentração  
Direito, Estado e Sociedade.

---

Norma Sueli Padilha, Dra.  
Coordenadora do Programa

---

Carolina Medeiros Bahia, Dra.  
Orientadora

Florianópolis, SC, 03 de março de 2020.

Ao João, por ser o melhor de mim, à Adriana, por ser comigo e aos meus pais, por serem por mim.

## **AGRADECIMENTOS**

A vida corre por caminhos incertos. Nela, o imponderável, o imprevisível, o surpreendente nos espera a cada nova pessoa que conhecemos. Algumas, desde o início da vida, outras desde pouco tempo, e muitas, independente do tempo, ocupam algum espaço afetivo dentro de nós. Afeto, assim como os dados, pode ser compartilhado sem perda.

Muitas pessoas foram fundamentais na trajetória que culmina nesse trabalho. A todas aquelas que, com pequenos gestos, generosas atitudes, sutis gentilezas, me ajudaram a concluir essa etapa, agradeço imensamente.

À minha orientadora, Profa. Carolina Bahia, agradeço por confiar em mim, desde o início e até o fim. Apendi muito contigo, dentro e principalmente fora da sala de aula. Porque grandes professores ensinam não só com giz e lousa, mas com atitudes. Sua coragem é inspiradora.

Às minhas sócias no escritório, Tatiana Braz Lux, Betânia Zardo e Lisandra Bornhausen, por terem equilibrado todos os pratos, sem deixar nenhum cair, no período de ausência para a conclusão deste trabalho. Betânia, obrigado pela revisão do primeiro capítulo. Foi uma ajuda e tanto! Tatiana, para você, um agradecimento mais do que especial, não apenas por todo apoio nesse período, que foi imenso, mas principalmente por compartilharmos valores e objetivos, desde o início.

Aos professores do Mestrado com os quais tive aula, obrigado pelos grandes ensinamentos. A todos os amigos que fiz aqui e que me ajudaram muito por todo esse período, em especial, Vivian De Gann, Ana Paula Varela, Amanda Burg, Isabela Sabo, Wanda Muniz Falcão, Victor Menezes e André Jannis, vocês são fantásticos!

Ao Prof. Everton das Neves Gonçalves, obrigado por todos os apontamentos realizados na minha qualificação. À Profa. Liz Sass, agradeço as observações feitas ao projeto e, principalmente, por ter lançado o desafio para um novo olhar sobre a questão da proteção de dados pessoais, mais crítica e que abordasse os problemas difíceis. Espero ter conseguido, pelo menos parcialmente, alcançar esse objetivo.

A Aline Irumé, colega da Comissão de Direito Digital, da OAB-SC, por identificar que não há muito conteúdo sobre aspectos técnicos, da computação, escrito em uma linguagem acessível aos profissionais do Direito. Espero que este trabalho, em algum grau, ajude a esclarecer conceitos e categorias importantes que, de alguma forma, estão ligados à proteção de dados pessoais.

A Reginaldo Pereira e Marcelo Markus Teixeira, obrigado por todo o apoio que vocês na graduação e, principalmente, pela amizade que nasceu em Chapecó e que seguirá viva, sempre. Agradeço também ao meu orientador, na graduação em Direito, Prof. Idir Canzi, por aceitar me orientar tendo como tema a proteção de dados pessoais, quando o assunto ainda não tinha a dimensão que tem hoje.

Ao meu grande amigo Maurício Campitelli Conti, obrigado pela presença constante em momentos decisivos da minha vida, nesses últimos 27 anos. É uma felicidade imensa poder conviver contigo.

A Paulo Henrique Ferreira, obrigado pelo incentivo e pelo entusiasmo de sempre em relação à vida acadêmica, sem perder de vista a prática profissional.

A Raphael Rocha Lopes, agradeço pelo apoio, desde o início, na atuação em Direito Digital. Sua experiência na advocacia me ensinou muito. Afinal de contas, para ser um bom advogado especialista em Direito Digital é preciso, antes, ser um bom advogado. E, nesse ponto, você foi e é um professor e tanto.

Como diz o João, meu filho, à minha grande família, meus pais, meus irmãos e cunhados e meus sobrinhos, obrigado pelo carinho e por serem sempre próximos, mesmo a milhares de quilômetros de distância.

Agora, para a minha pequena família, Adriana e João, as palavras ficam pequeninhas perto do tamanho da minha gratidão, principalmente por esses últimos quatro meses. Foi um grande período de ausência, mesmo que fisicamente nos víssemos diariamente. Vencida essa etapa vamos passar muito mais tempo juntos. Amo muito vocês.

João, agora dá para dizer: o papai acabou!

*"Deus move o jogador, e este, a peça.  
Que deus detrás de Deus o artilheiro começa  
de pó e tempo e sonho e agonias?"  
(Jorge Luis Borges, 1960)*



## RESUMO

Plataformas digitais, estruturadas como mercados de dois ou múltiplos lados, onde o consumidor não paga, em dinheiro, para acessá-las, são utilizadas diariamente por bilhões de pessoas espalhadas pelo mundo. Movidas por um imenso poder computacional, vendem a atenção das pessoas a anunciantes, em complexos sistemas de leilão de espaços publicitários ultra segmentados, que buscam incessantemente a individualização do alvo e cuja precisão está diretamente ligada à imensa quantidade de dados pessoais capturados e associados a cada pessoa que as utilizam, o que as transformam em grandes máquinas de vigilância, ameaçando os Direitos Fundamentais relacionados à proteção de dados pessoais. Este trabalho apresenta uma proposta de regulação que objetiva elevar o nível de proteção dos Direitos Fundamentais ligados à proteção de dados pessoais dos usuários pela vedação à gratuidade compulsória desses serviços. Para tanto, analisa as plataformas digitais por três diferentes prismas: a) os elementos articulados em seu funcionamento: poder computacional, dados pessoais, tempo e conteúdo dos outros; b) as três posições simultâneas ocupadas pelos indivíduos, em um processo circular, ao utilizá-las: consumidor, fornecedor de matéria-prima e produto e c) as externalidades positivas aproveitadas pelas plataformas para fixarem posições dominantes no mercado e até se consolidarem como monopólios. O trabalho também apresenta os limites das legislações de proteção de dados, como a Regulamento Geral de Proteção de Dados (GDPR) europeia e a Lei Geral de Proteção de Dados - Lei 13.709/2018 (LGPD) brasileira, além da necessidade de se articular outros mecanismos jurídicos como o Direito do Consumidor e o Direito Antitruste para, de forma conjunta, aumentar a eficácia dos Direitos Fundamentais. Por fim, apresenta a sugestão de regulação, onde as plataformas passariam a ser obrigadas a disponibilizar uma opção de oferta em que o consumidor pagaria, em dinheiro, para utilizá-las, vedando a utilização dos dados pessoais e da atenção dos usuários para fins próprios da plataforma ou de terceiros, como forma de minimizar o tratamento desses dados e, conseqüentemente, aumentar o nível de proteção dos direitos da personalidade dos usuários consumidores. Para tanto, adotou-se como método de procedimento o funcionalista, como método de abordagem o dedutivo e como técnicas as pesquisas bibliográfica e documental.

**Palavras-chave:** Proteção de dados pessoais. Plataforma de dois lados. Regulação.

## ABSTRACT

Digital platforms, structured as two, or multiple sided markets, where consumers do not pay, in cash, to access them, are used daily by billions of people around the world. Driven by immense computational power, they sell people's attention to advertisers on complex auction systems for ultra-targeted advertising spaces, that constantly seek to individualize the target and whose accuracy is directly linked to the immense amount of personal data captured and associated with each user. This process turns those Platforms into great surveillance machines, threatening the Fundamental Rights related to the protection of personal data. This work presents an application proposal that aims to raise the level of protection of Fundamental Rights linked to the protection of users' personal data based on the prohibition of compulsory gratuity of these services. To do so, analyze digital platforms through three different approaches: a) their functional elements: computational power, personal data, time and content of others; b) the three simultaneous positions occupied by individuals, in a circular process, when using them: consumer, supplier of raw materials and product; and c) the positive externalities used by the platforms to establish dominant positions in the market and even consolidate themselves as monopolies. The work also presents the limits of data protection legislation, such as the European General Data Protection Regulation (GDPR) and the Brazilian General Data Protection Law (LGPD), in addition to the need to articulate other legal mechanisms such as Consumer and Antitrust Laws to jointly increase the strength of the Fundamental Rights. Finally, it suggests a regulation where platforms would be obliged to offer a cash paid option that would prohibit the use of personal data and the attention of users for the purposes of the platform or third parties, as a way to minimize the processing of this data and, consequently, increase the level of protection of the users' personality rights. This work adopts the functionalist procedure method, the deductive approach method and the bibliographic and documentary research techniques.

**Keywords:** Personal data protection. Two-sided Platforms. Regulation.

## LISTA DE FIGURAS

Figura 1 – Aplicativos de Mapas mais Populares nos Estados Unidos em Abril de 2018, por alcance. . . . .	32
Figura 2 – Arquitetura de infraestrutura IoT. . . . .	41
Figura 3 – A netoide se ajusta bem aos dados de crescimento de usuários do Facebook, medidos em termos de usuários médios mensais (MAUs), e a lei da Metcalfe se ajusta bem aos dados de receita do Facebook.	97
Figura 4 – Desenho esquemático da relação geral entre erro e volume de dados utilizados no treinamento de aplicações de inteligência artificial. . . . .	114
Figura 5 – Diagrama de interação entre os múltiplos lados, no modelo de negócio do Facebook . . . . .	146
Figura 6 – The Washington Post: página de assinatura para a Europa . . . . .	175

## LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AEPD	Agencia Española de Protección de Datos
ANPD	Autoridade Nacional de Proteção de Dados
API	Interface de Programação de Aplicação
AWS	Amazon Web Services
CCPA	California Consumer Privacy Act
CDC	Código de Defesa do Consumidor
cgi.br	Comitê Gestor da Internet no Brasil
CNAE	Cadastro Nacional de Atividade Econômica
CNIL	Commission Nationale de l'Informatique et des Libertés
CNPJ	Cadastro Nacional de Pessoa Jurídica
CRM	Customer Relationship Management
DaC	Dados como Capital
DaL	Dados como Trabalho
DMP	Data Marketplace
DPO	Data Protection Officer
EDPB	Comitê Europeu para a Proteção de Dados
EDPS	Autoridade Europeia de Proteção de Dados
EUA	Estados Unidos da América
GDPR	Regulamento Geral de Proteção de Dados
GUI	Interface Gráfica do Usuário
GWB	Lei de Competição da Alemanha
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IA	Inteligência Artificial
IaaS	Infraestrutura como Serviço
IAPP	Associação Internacional dos Profissionais de Privacidade
IBGE	Instituto Brasileiro de Geografia e Estatística
ICO	Information Commissioner's Office
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet das Coisas
LGPD	Lei Geral de Proteção de Dados - Lei 13.709/2018
MEI	Microempreendedor Individual
nic.br	Núcleo de Informação e Coordenação do Ponto BR
PaaS	Plataforma como Serviço
PC	Computador Pessoal
PEC	Proposta de Emenda à Constituição
PIMS	Sistemas de Gerenciamento de Informações Pessoais

SaaS	Software como Serviço
SEO	Search Engine Optimization
UBI	Renda Básica Universal
UFSC	Universidade Federal de Santa Catarina
VRM	Vendor Relationship Management
WP29	Grupo de Trabalho do Artigo 29.º
XML	Extensible Markup Language

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>15</b>
<b>2</b>	<b>PODER COMPUTACIONAL, TEMPO, DADOS PESSOAIS E CONTEÚDO DOS OUTROS</b>	<b>20</b>
2.1	<i>AO NOSSO LADO, TEMOS A LEI DE MOORE</i>	22
2.1.1	<b>Latifúndios computacionais</b>	<b>24</b>
2.1.2	<b><i>Cookies</i>, Interface de Programação de Aplicação (API)s e <i>Open Source</i></b>	<b>33</b>
2.1.3	<b>Transistores e sensores em todos os lugares</b>	<b>37</b>
2.2	<i>UM ALVO SEMPRE NA MIRA</i>	45
2.2.1	<b>A economia do encontro</b>	<b>46</b>
2.2.2	<b>Da economia do encontro à economia da vigilância</b>	<b>51</b>
2.2.3	<b>Quem paga pelo tempo livre?</b>	<b>56</b>
2.3	<i>NÓS NÃO VAMOS PAGAR NADA, É TUDO FREE</i>	61
2.3.1	<b>Apropriação de conteúdo</b>	<b>62</b>
2.3.2	<b>Nossa vida como conteúdo</b>	<b>68</b>
<b>3</b>	<b>CONSUMIDOR. MATÉRIA-PRIMA. PRODUTO.</b>	<b>73</b>
3.1	<i>GRATUIDADE, CONCENTRAÇÃO DE PODER E O MERCADO DE UM</i>	74
3.1.1	<b>A economia da privacidade</b>	<b>76</b>
3.1.2	<b>Plataformas, mercados de dois lados e monopólio</b>	<b>84</b>
3.1.2.1	Efeitos de rede e competição	87
3.1.2.2	<i>Data-driving network effects</i>	89
3.1.2.3	Preço zero do lado do usuário	91
3.1.2.4	Lei de Metcalfe e o efeito de rede	94
3.2	<i>PERSONALIDADE COMO MERCADORIA SEM PREÇO</i>	98
3.2.1	<b>A dupla face dos dados pessoais e a sua proteção constitucional</b>	<b>98</b>
3.2.1.1	Bens não rivais, propriedade e acesso	100
3.2.1.2	Proteção de dados pessoais como garantia constitucional	107
3.3	<i>CONSUMIDOR EMPACOTADO E ENTREGUE</i>	112
<b>4</b>	<b>DESARMANDO A ARMADILHA DA GRATUIDADE ENGANOSA</b>	<b>116</b>
4.1	<i>UM PROBLEMA GRANDE DEMAIS PARA AS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS</i>	117
4.1.1	<b>Repensar a privacidade e a proteção de dados como um todo?</b>	<b>119</b>
4.1.2	<b>Uma visão crítica sobre a GDPR</b>	<b>128</b>
4.1.2.1	A amplitude dos conceitos de dados pessoais e de tratamento de dados pessoais	128
4.1.2.2	Como identificar o responsável, se a responsabilidade é de todo mundo?	138

4.1.2.3	Foco no <i>compliance</i> e não na proteção de dados pessoais . . . . .	140
4.2	DIREITO DO CONSUMIDOR E CONCORRENCIAL NA DEFESA DOS DIREITOS FUNDAMENTAIS . . . . .	142
4.2.1	<b>A simbiose entre Proteção à Concorrência e Proteção de Dados Pessoais . . . . .</b>	<b>144</b>
4.2.1.1	Novos parâmetros para a proteção à competição . . . . .	151
4.2.2	<b>Direito do Consumidor e seu papel na extensão da proteção dos Direitos Fundamentais . . . . .</b>	<b>157</b>
4.2.2.1	Simulacro da remuneração indireta e práticas abusivas . . . . .	159
4.3	<i>LIBERDADE PARA PAGAR</i> . . . . .	167
4.3.1	<b>Definindo os alvos da regulação . . . . .</b>	<b>169</b>
4.3.2	<b>No mercado, tudo tem um preço . . . . .</b>	<b>171</b>
4.3.2.1	Precificação indireta dos dados pessoais . . . . .	173
4.3.2.2	Os contornos da vedação à gratuidade compulsória . . . . .	177
4.3.3	<b>Ganhos potencialmente gerados pelo fim da gratuidade compul- sória . . . . .</b>	<b>181</b>
4.3.4	<b>Limitações do modelo . . . . .</b>	<b>184</b>
5	<b>CONCLUSÃO . . . . .</b>	<b>186</b>
	<b>REFERÊNCIAS . . . . .</b>	<b>190</b>
	<b>ANEXO A – RELATÓRIO DE VARREDURA DE <i>COOKIES</i> . . . . .</b>	<b>209</b>

## 1 INTRODUÇÃO

Ireneu Funes nasceu e morreu em Fray Bentos<sup>1</sup>, capital do departamento de Río Negro, a 360 quilômetros de Montevideu, no Uruguai. Aos dezenove anos, em um acidente a cavalo, perdeu os movimentos do corpo, mas ao mesmo tempo passou a ter percepção e memória absolutas. Nada lhe passava despercebido. Capturava tudo, por todos os sentidos, nos mínimos detalhes, e se lembrava de tudo, inclusive dos momentos em que passou lembrando de um fato específico, por menor que fosse, como um movimento inesperado de uma folha em uma árvore avistada da janela do seu quarto. Segundo o relato ficcional de Borges, “[s]abia as formas das nuvens austrais do amanhecer do dia 30 de abril de 1882 e podia compará-las na lembrança com os veios de um livro em papel espanhol que ele havia olhado uma única vez”. Mas soterrado por tantos detalhes e nunces não conseguia fazer uma abstração, uma generalização sequer, o que levou Borges a concluir, depois da conversa que tiveram em 14 de fevereiro de 1887, que Funes era incapaz de pensar. Mesmo assim, sentiu medo só de saber que todas as suas palavras e todos os seus gestos seriam guardados, para sempre, em uma memória infalível (BORGES, 1996).

Agora, em um exercício criativo adicional, e se imaginássemos que Funes fosse, ao mesmo tempo, dois? Um capaz de capturar e armazenar tudo e outro com o poder de selecionar, dessas memórias infinitas, aquelas que são verdadeiramente úteis para uma determinada finalidade? Talvez, nesse caso, teria razão Pedro Leandro Ipuche<sup>2</sup> que considerava Funes o precursor dos super-homens (BORGES, 1996). Agora, continuando o exercício, e se alguém pudesse controlar Funes? Capturar e utilizar suas sensações e memórias, com tempo e capacidade para selecionar e organizar as informações para algum fim útil? Seria uma vantagem, para o controlador, é claro, mas que possui uma grande limitação. Preso ao catre, Funes não consegue ver mais do que o alcance da vista lançada pela janela do seu quarto. Mas e se fosse possível controlar mais de um Funes? E se Funes fosse tão pequeno que coubesse em todos os lugares? E se fosse possível controlá-los aos bilhões?

Na economia da vigilância, ao redor de cada pessoa orbita diversos Funes, cada um observando e percebendo uma nuance diferente de comportamento, no mundo real e também na Internet, gerando memórias para alguém que poderá utilizá-las inteligentemente. Mas ao contrário de Borges, que percebe vivamente o poder da memória infinita e sente medo, os Funes da vida real passam despercebidos, mudos, quase invisíveis e geralmente entram no cotidiano das pessoas acompanhados por algum benefício atraente, como a possibilidade de utilizar um serviço útil ou prazeroso

<sup>1</sup> As informações sobre Fray Bentos foram retiradas da enciclopédia Borges Babilônico, de vertebre específico sobre a cidade (ROCCA; BRIZ, 2017a)

<sup>2</sup> Apesar de participar de um relato ficcional, Pedro Leandro Ipuche existiu na realidade. Poeta, narrador e ensaísta uruguaio, viveu entre 1889 e 1976 (ROCCA; BRIZ, 2017b)



sem ter que desembolsar nenhum centavo.

Apesar de estarem sempre a espreita, muitas vezes memorizando o que não lhes seria permitido, já não é possível eliminar os Funes. Eles se espalham por todos os lados e se multiplicam exponencialmente. Mas talvez o gênio de Borges possa apontar uma saída. Funes, sozinho, pouco ou nada pensa, por isso é praticamente inofensivo. Uma alternativa para minimizar a vigilância pode passar não por eliminá-los, mas por desconectá-los da inteligência central.

Este trabalho segue, exatamente, essa linha e tem como objetivo apresentar uma proposta de regulação que busca elevar o nível de proteção dos Direitos Fundamentais ligados à proteção de dados pessoais dos usuários a partir da vedação à gratuidade compulsória das plataformas digitais, tendo como premissa que, não sendo obrigado a ceder seus dados pessoais, para uso em fins próprios da plataforma ou de terceiros, em troca da utilização dos serviços, há o aumento do poder de disposição, dos indivíduos, sobre seus próprios dados, e a mitigação dos efeitos perniciosos da economia da vigilância, pela diminuição dos dados disponíveis para a realização de atividades de perfilização destinadas à segmentação de publicidade e à realização de ações de marketing comportamental.

Os três objetivos secundários, dispostos nos dois primeiros capítulos, referem-se à análise dos elementos essenciais envolvidos no modelo de negócio das plataformas digitais; à descrição das posições ocupadas pelos usuários, simultaneamente, na utilização destes serviços e à análise das externalidades positivas, aproveitadas pelas plataformas, para atingirem posições dominantes de mercado.

No Capítulo 2, inicia-se a abordagem dos quatro elementos articulados pelas plataformas digitais para implementarem seus modelos de negócio: grande poder computacional, organizado de modo complexo, por imensos emaranhados de infraestruturas e aplicações, em diversos níveis, que se misturam, se complementam e se expandem em imensas teias, com grande capilaridade, capazes de capturar informações sobre os movimentos, sensações e sentimentos das pessoas, muitas vezes sem serem sequer percebidas; o tempo, que ultrapassa os limites daquela fração dispendida pelo usuário no uso direto da aplicação e que é apropriado utilizando-se a rede capilar de captação de dados existente nas pontas destas super estruturas computacionais e, por fim, o conteúdo gerado por terceiros e utilizado livremente pelas plataformas, sem que estas paguem por isso, mas que, depois de processado, é firmemente protegido, em um modelo de transformação de bem público em bem privado, que também é abordado.

O Capítulo 3 traz os dados pessoais como o quarto elemento essencial para o funcionamento das plataformas e apresenta a segunda perspectiva, vista a partir do usuário e das três posições que ocupa, simultaneamente e de forma circular, na interação com esses serviços. A primeira dimensão, mais evidente, é a do consumidor

que utiliza um serviço de um fornecedor, em uma clássica relação de consumo. Na segunda, o indivíduo posiciona-se como fornecedor de matéria-prima, já que seus dados pessoais são captados, como uma forma de contraprestação pelos serviços usufruídos, e utilizados como insumo para outra relação contratual, estabelecida simultaneamente pela plataforma com os anunciantes, que desejam atingir os usuários com maior propensão de compra para os produtos que oferecem. Para ajustar esse alvo, todas as engrenagens computacionais e de captação de dados pessoais são movimentadas no sentido de criar perfis cada vez mais individualizados, na busca do ideal mercado de um, onde o excedente do lado do consumidor é zero. Na terceira, como verdadeiros alvos da publicidade personalizada, engendrada pelo marketing comportamental (*behavior marketing*), os usuários se transformam em produtos leiloados aos anunciantes. Também neste capítulo, aborda-se a terceira perspectiva da análise das plataformas, ligada à economia da privacidade e às externalidades positivas aproveitadas por elas para atingirem posições dominantes, em alguns casos, se transformando em monopólios.

Já no último capítulo, aborda-se a fragilidade das legislações específicas de proteção de dados pessoais para lidarem, sozinhas, com as ameaças trazidas pelas plataformas aos Direitos Fundamentais, a partir de duas abordagens: uma estrutural, que questiona algumas categorias relevantes dos sistemas de proteção de dados, e outra voltada às dificuldades de aplicação das normas, principalmente quanto à eficácia frente às plataformas que operam em dois ou múltiplos lados. Como alternativa a estas fragilidades, apresenta-se a necessidade de articulação com outros mecanismos normativos, como o Direito do Consumidor e o Direito Concorrencial, alimentando um debate já existente na Europa sobre o tema e contextualizando-o para o Brasil, sempre que possível. Segue-se, então, para um aprofundamento das possíveis contribuições trazidas por estas duas áreas, separadamente consideradas, para o aumento da proteção dos Direitos Fundamentais, a partir da possibilidade de criação de limites mais claros para o tratamento de dados pessoais, de modo a refrear a economia da vigilância. Na parte final, apresenta-se uma sugestão de regulação, baseada na vedação à gratuidade compulsória dos serviços digitais, abrindo a possibilidade de escolha, pelo consumidor, de não ceder, como forma de remuneração direta, seus dados pessoais para tratamentos baseados no legítimo interesse da plataforma ou de terceiros. Conclui-se com a apresentação dos potenciais ganhos gerados por esta opção de regulação e, também, aponta-se três dos seus principais pontos fracos.

Infelizmente, o Brasil não possui uma cultura de proteção de dados pessoais. Esse traço se tornou evidente com o fracasso retumbante do *habeas data* como remédio constitucional, como já previa Barbosa Moreira (1998), e pela decisão da Assembleia Nacional Constituinte de retirar, do texto final, a previsão expressa da proteção de dados pessoais do rol dos direitos fundamentais (SILVA, 1994). Por esse motivo, em

diversas circunstâncias, os casos apresentados e as legislações abordadas têm origem europeia, onde a estrutura normativa específica sobre o tema evoluiu há décadas e onde as decisões dos tribunais e os pronunciamentos das autoridades de proteção de dados dão contornos mais claros à legislação. A opção por uma visão europeia se dá pelo fato de que, optou-se, no Brasil, pela criação de uma lei geral de proteção de dados com sólidas raízes no modelo europeu. Sempre que possível, os exemplos foram contextualizados para a realidade brasileira.

Do ponto de vista metodológico, como método de procedimento optou-se pelo funcionalista, devido à lógica de ações e reações ocorridas na trama social, que geram ações e reações institucionais (MEZZAROBÀ; MONTEIRO, 2017), inerente a qualquer abordagem regulatória e, também, pela existência de funções latentes (LAKATOS; MARCONI, 2017), tendo em vista que diversas das relações envolvendo dados pessoais são invisíveis aos indivíduos que interagem e cedem seus dados para uso, pelas plataformas, para seus próprios fins, principalmente utilizados como insumo em outras cadeias de negócios jurídicos, realizados, em geral com outras empresas, nos demais lados do mercado de múltiplos lados. Como método de abordagem, optou-se pelo dedutivo, com hipótese de pesquisa sendo estabelecida, em *modus ponens*, nos seguintes termos: se não há gratuidade compulsória (premissa antecedente), eleva-se o nível de proteção dos dados pessoais (premissa consequente). A gratuidade compulsória é vedada. Eleva-se o nível de proteção de dados pessoais. Já como técnica de pesquisa, foram utilizadas a pesquisa bibliográfica, baseada na doutrina, e a pesquisa documental, com foco na legislação, na jurisprudência e em matérias jornalísticas, além de contratos, termos de uso e políticas de privacidade relacionadas a serviços digitais.

Algumas considerações adicionais são necessárias. Como tudo o que articula tecnologia e aspectos da vida humana, ao passar das páginas o leitor sentirá as marcas do tempo em que elas foram escritas. Essa impressão digital do tempo do autor é implacável e não se afasta, sequer, dos melhores autores de ficção científica. Os vestígios, portanto, do início da segunda década do século XXI estão espalhadas por todos os lados.

Apesar de um olhar prospectivo, que busca aumentar o nível de proteção dos Direitos Fundamentais em um mundo cada vez mais mediado por plataformas digitais, esse trabalho também se volta ao passado. Grande parte das decisões que moldaram a realidade quotidiana de hoje, onde a vida transpassa, ininterrupta e quase que imperceptivelmente, do ambiente digital para fora dele e a ele retorna, em uma acelerada rotina de Sísifo, foram tomadas ainda no século passado, mais precisamente na segunda metade dos anos noventa, e nos primeiros anos desse século. Já os alicerces que sustentaram essas decisões vêm sendo construídos há mais tempo, a partir do início da segunda metade do século XX. Para dar melhores contornos ao contexto

atual, resgata-se, principalmente no primeiro capítulo, mas também em alguns outros pontos dispersos, um pouco desse passado.

Não se deve perder de vista que ambientes digitais são construídos, essencialmente, por cientistas da computação, engenheiros, matemáticos, físicos, ou seja, pelo pessoal das exatas. Entender como essas pessoas pensam é imprescindível para entender o contexto tecnológico. Não é apenas no retorno de 42, dentro de uma calculadora, numa busca no Google por ‘resposta para a vida o universo e tudo mais’, ou no uso recorrente de emojis, que são derivados de expressões em ASCII<sup>3</sup> ( :- ) , :-D , :-b , <3 ) ou, ainda, no uso recorrente das *#hashtags*, que foram originalmente pensadas como uma forma de facilitar a identificação de conteúdo específico em uma fonte de dados não estruturada, como o Twitter, mantendo a contextualização da comunicação (MESSINA, 2007), que as influências técnicas e da cultura nerd se materializam. Diversas decisões de investimento, projeto e modelagem de negócios baseiam-se nesse modo de pensar orientado pela computação e pela matemática. Dar voz a algumas dessas pessoas, primeiro traz uma dimensão humana a algo que, muitas vezes, é considerado apenas interações com máquinas, e, principalmente, expõe perspectivas, com efeitos concretos, que não são percebidas por olhares vindos de outras áreas, como o Direito. Em vários momentos, ouve-se a voz dessas pessoas, algumas por meio de longas citações, para que o tom e as nuances não sejam perdidas, mais do que foram no processo de tradução.

Este trabalho conecta três grandes áreas do conhecimento e, de cada uma, herdou um conceito seminal. Da ciência da computação, o reconhecimento da importância e da volatilidade dos dados. Da economia, a dinâmica dos mercados. E do Direito, a compreensão da importância dos Direitos Fundamentais e do dever de protegê-los. Observar os problemas jurídicos no ambiente digital passa, de modo inescapável, por estas três áreas, tendo em vista que, enquanto se deseja aumentar a eficácia dos Direitos Fundamentais, o fluxo de dados acelera, impulsionado pelo caráter exponencial da capacidade de processamento de informações, o que acentua a concentração de poder computacional e, conseqüentemente, a influência política dos donos desse poder, que pode afetar a conformação dos mercados. Neste sentido, é preciso manter-se sempre atento e disposto a experimentar, ao menos conceitualmente, novos paradigmas, pois os modelos jurídicos adotados hoje poderão não ter lugar, por completa ineficácia, no mundo do próximo ciclo tecnológico.

<sup>3</sup> *American Standard Code for Information Interchange* ou Código Padrão Americano para o Intercâmbio de Informação, traz uma relação de símbolos gráficos, com códigos binários associados, utilizados em interfaces de texto, dentre outras aplicações.)

## 2 PODER COMPUTACIONAL, TEMPO, DADOS PESSOAIS E CONTEÚDO DOS OUTROS

O despertador toca. Na verdade, o volume vai subindo suavemente e a voz de Vanessa Carlton, cantando *A Thousand Miles* vai preenchendo o quarto até o ponto em que é impossível manter o sono. Essa escolha não foi por acaso. É a música preferida de uma lista com 21 canções selecionadas, como as melhores para se acordar, pelo psicólogo David M. Greenberg e pelo time de dados do aplicativo Spotify, por ter uma "construção lenta, uma mensagem positiva e uma batida forte"(DARRISAW, 2019). Pelo menos era isso que dizia a matéria, no OprahMag.com.

Quando o som chega ao máximo, o braço alcança o celular e desativa o despertador do aplicativo de relógio que estava conectado ao Spotify, aquele mesmo aplicativo que ajudou o Dr. Greenberg a fazer a sua lista de melhores músicas para acordar. Com o polegar, o relógio é jogado de lado e logo aparecem na tela as últimas atualizações do WhatsApp. Nas conversas fixadas<sup>1</sup>, nenhuma mensagem nova, o que já traz um certo alívio. Nenhuma mensagem de alguém importante. Nos grupos, a noite foi agitada, mesmo depois das três da manhã, horário da última consulta ao aplicativo, em um momento de perda de sono. Uma passada rápida pelos principais, só para ver em que ponto pararam as conversas, e o dedo desliza, mais uma vez, trocando o WhatsApp pelo Instagram.

De quinze a vinte roladadas de tela, com movimentos constantes do polegar, na vertical, de baixo para cima, é suficiente para ver como foi a noite e a madrugada dos outros. Muitos conhecidos, alguns estranhos, todos em momentos fantásticos de alegria e êxtase, mas só alguns poucos merecedores de um coraçãozinho de *like*. Claro, tudo intercalado com alguns posts de autoajuda e outros tantos de propaganda. Rapidamente, o dedo toca o segundo círculo com fotos no topo da tela e os *stories* começam a rodar. Em um ritmo geralmente mais lento do que a paciência, a cada 2 ou 3 segundos um novo toque de tela faz pular de um vídeo para outro, bem antes do fim. E lá se vão mais uns 30 ou 40 toques.

Mais alguns movimentos e o Instagram dá lugar ao Facebook. Lá se foram mais de 10 minutos. A luz do quarto ainda está apagada, o corpo coberto, só um pouco recuado, no sentido da cabeceira da cama, a ponto da cabeça se dobrar o suficiente para que os olhos se emparelhem com o aparelho mantido na vertical. Aquela sensação de perda de tempo começa a aparecer. "O que as pessoas fazem ainda no Facebook?", pensa enquanto rola o *feed* sem prestar muita atenção. O tempo aperta e a ansiedade, logo cedo, já espreita o quarto, mesmo antes de a luz estar acesa. É hora do GMail. Começa limpando os spams e passando os olhos, rápidos, pelas newsletters e pelas

<sup>1</sup> "A ferramenta fixar conversa lhe permite colocar até três conversas específicas no topo da sua lista de conversas. Conversas que foram fixadas estarão sempre ao topo da lista para que você tenha acesso rapidamente quando quiser acessá-las.", FAQ do WhatsApp. URL: [https://faq.whatsapp.com/pt\\_br/android/26000047/?category=5245251](https://faq.whatsapp.com/pt_br/android/26000047/?category=5245251) . Acessado em 12 nov. 2019.

listas de *to dos* e compromissos do dia. Tirando isso, não sobra quase nada. Afinal de contas, quem envia e-mail ainda?

Pronto! Depois de quase 20 minutos, talvez um pouquinho mais, volta ao relógio. Não vai dar tempo de tomar café. O braço se estica novamente. A luz se acende. É hora de escovar os dentes e começar o dia.

Esse relato é ficcional, mas está aqui porque reflete uma realidade que levou à eleição, em votação popular realizada pelo Cambridge Dictionary, em 2018, de *nomophobia*<sup>2</sup> como palavra do ano. Em português, a palavra já aparece catalogada no Dicionário Michaelis, como termo relacionado a medicina e psicologia, com o seguinte significado: "medo mórbido de ficar sem celular e, em decorrência disso, incomunicável com o mundo. Esse tipo de fobia pode provocar dor de cabeça, falta de ar, ansiedade e taquicardia."(EDITORA MELHORAMENTOS, 2015).

Em 2016, a consultoria Deloitte, em uma série de pesquisas denominada *Global Mobile Consumer Survey* (DELOITTE, 2016) constatou que da amostra ouvida na pesquisa, 32% das pessoas que possuíam *smartphones* declararam que sua primeira ação ao acordar era olhar o aparelho, enquanto 48% destas pessoas olham o celular, uma última vez, até cinco minutos antes de dormir. A mesma pesquisa, no ano seguinte, constatou que, do espaço amostral, 14% dos respondentes acordavam durante a noite para conferir o telefone (DELOITTE, 2018). Já em 2019, 81% dos entrevistados declararam consultar suas mensagens no aplicativo WhatsApp pelo menos a cada hora. Outros 16% declararam consultar o aplicativo uma vez por dia, o que soma 97% (DELOITTE, 2019) do total de respondentes. O brasileiro com acesso, em média, utiliza a Internet por 9 horas e 29 minutos, sendo que deste tempo, 3 horas e 34 minutos são dispendidos em redes sociais. Somos o segundo país do mundo que gasta mais tempo na internet, atrás apenas das Filipinas, enquanto a média mundial é de 6 horas e 42 minutos. Já a população de países como Bélgica, Suíça, Holanda, França, Alemanha e Japão gasta, em média, menos de 5 horas do seu dia conectada (KEMP, 2019).

Os hábitos de uso desta personagem não se distanciam do perfil de uso da população brasileira. Segundo a Pesquisa Nacional de Amostra de Domicílios Contínua, realizada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2017, 95,5% do total de usuários da internet acessavam a rede com a finalidade de enviar ou receber mensagens de texto, voz ou imagem por aplicativos diferentes do e-mail. Já 81,8% utilizavam para assistir vídeos, enquanto 83,8% utilizavam para fazer chamadas de voz ou vídeo e 66,1% para enviar e receber e-mail. Até o comentário sobre o uso do e-mail é pertinente: ao se comparar os dados de 2017 com os de 2016, observa-se

<sup>2</sup> O verbete *nomophobia*, no Cambridge Dictionary possui o seguinte significado "fear or worry at the idea of being without your mobile phone or unable to use it"(CAMBRIDGE DICTIONARY, 2018). Já no Oxford Dictionary, onde foi catalogado em 2019, *nomophobia* possui dois significados, um alinhado com o sentido apresentado pelo Cambridge Dictionary, literalmente, "anxiety about not having access to a mobile phone or mobile phone services", mas também, em sentido adicional, "aversion to or fear of laws or rules"(OXFORD ENGLISH DICTIONARY, 2019).

uma redução de 3,2% no uso da internet para essa finalidade (IBGE, 2018).

Dois características marcam, de forma preponderante, as aplicações utilizadas pelo usuário arquetípico apresentado neste capítulo. A primeira refere-se ao fato de que todas elas se auto declaram como *gratuitas* para seus usuários, fato que, na verdade, distancia-se da realidade e que será alvo de uma ampla abordagem no terceiro capítulo desta dissertação.

A segunda relaciona-se à forma como combinam quatro elementos fundamentais, cuja articulação, em grande medida, marca o *modus operandi* destas aplicações: alto poder computacional; captura do tempo dos usuários; apropriação de conteúdos gerados por terceiros como parte (ou quase a totalidade) de suas ofertas e coleta e processamento de grandes volumes de dados pessoais.

Neste capítulo, será realizada a análise dos três primeiros elementos. Já o capítulo dois será dedicado à análise dos aspectos ligados aos dados pessoais dos usuários de aplicações alegadamente disponibilizadas gratuitamente, partindo-se das três posições ocupadas por uma pessoa quando utiliza este tipo de aplicação: consumidor, a posição mais óbvia; fonte de matéria-prima, tendo em vista que seus dados pessoais são utilizados como insumo para as ofertas de produtos de publicidade e marketing disponibilizados pelas plataformas e, por último, na posição de produto, entregue aos anunciantes como público alvo altamente segmentado, sobre o qual a mensagem publicitária tem maiores chances de ser convertida em venda.

## 2.1 AO NOSSO LADO, TEMOS A LEI DE MOORE

Em uma manhã de 1998, David Cheriton, professor de Ciência da Computação na Universidade de Standord, abriu sua casa para promover um encontro que mudaria a história da internet e, conseqüentemente, a maneira como vivemos e organizamos os meios de produção, em uma economia essencialmente orientada a dados.

Na varanda da casa de Cheriton, dois alunos de doutorado, Lerry Page e Sergey Brin, que, coincidentemente, foram para Stanford depois de serem rejeitados no processo seletivo do MIT (Massachusetts Institute of Technology), esperavam a chegada de um dos mais respeitados investidores-anjo do Vale do Silício, Andy Bechtolsheim (VISE; MALSEED, 2018).

Bechtolsheim não era apenas um investidor. Era, acima de tudo, um engenheiro com contribuições singulares à computação. Ainda como estudante de doutorado, no início da década de 1980, juntamente com Forest Basklett e Vaughan Pratt, concebeu a ideia de uma estação de trabalho. A SUN (acrônimo para *Stanford University Network*) Workstation era, nas palavras de seus próprios criadores, "um computador pessoal que combina capacidades gráficas e de rede com poderoso processamento local"(BECHTOLSHEIM; BASKETT; PRATT, 1982)<sup>3</sup>. Sua arquitetura e a utilização de

<sup>3</sup> Ao incluir esta referência na dissertação, o autor desse trabalho postou, em sua *timeline* no Facebook,

componentes de baixo custo, em grande medida, serviram de base para o que se designaria, futuramente, como Computador Pessoal (PC), e talvez mais do que os próprios PCs, foi responsável pelo fim dos caros mini-computadores da IBM, DEC e Wang, além dos mainframes que dominavam a indústria (MYERS, 2012).

Page e Brin não estavam buscando dinheiro para investimentos em marketing e também não tinham apenas uma ideia descrita em uma apresentação de PowerPoint. O mecanismo de busca que eles criaram já funcionava e precisavam levantar dinheiro para comprar os componentes, que permitiriam que eles próprios construíssem os computadores que sustentariam a até então lunática fantasia de fazer uma cópia de toda a web. Em uma apresentação do seu mecanismo de busca, em Stanford, a convite do professor Dennis Allison, ao ser indagado sobre a viabilidade da empreitada, tendo em vista que a própria internet crescia (e cresce) de forma acelerada, Brin respondeu: "Então, como você faz isso? Bem, acontece que não é tão ruim. Do nosso lado, temos a Lei de Moore<sup>4</sup><sup>5</sup> (VISE; MALSEED, 2018). Esta busca por tentar resolver o impossível sempre foi uma marca de Page e Brin. O próprio Bechtolsheim, mais tarde, ao analisar a cultura de inovação das grandes empresas de tecnologia americanas, reconheceria esta marca característica do Google, juntamente com uma forma agressiva de estabelecer metas em grande escala, desenvolver ideias mais rápido que os outros e contratar pessoas inteligentes e tratá-las bem (BECHTOLSHEIM, 2012).

A finalidade do investimento criava, com Bechtolsheim, um ponto de contato. A dupla, naquele momento, precisava de dinheiro para construir computadores de baixo custo e começaram isso nos laboratórios de Stanford. Uma geração antes, nos mesmos corredores e salas, mais precisamente em 1.979, Bechtolsheim teve acesso à placa com processador Motorola 68000, o primeiro microprocessador de 32 bits. Nos meses seguintes, construiu uma placa Ethernet (para comunicação em rede) e uma placa gráfica que controlava um monitor preto e branco. Assim, construiu sua primeira estação de trabalho (FAIRBAIRN, 2015).

Mas havia algo fundamental que diferenciava as duas iniciativas. Enquanto Bechtolsheim via um grande potencial comercial na venda destes computadores, o que culminou na criação da Sun Microsystems, em 1982, Brin e Page não queriam vender diretamente poder de processamento, mas sim utilizá-lo para sustentar uma ousada iniciativa de processamento de informações, organizando dados não estruturados de forma a tornar todo o conhecimento humano, até então disponibilizado via internet,

---

uma foto da capa original do relatório que descreve a arquitetura da SUN Workstation. Poucos minutos depois, o atento Dr. Paulo Lício de Geus, professor livre-docente da Universidade Estadual de Campinas (UNICAMP), identificou um erro de grafia, no nome de Bechtolsheim, onde a letra l dá lugar, equivocadamente, a uma letra t. Fica, nessa nota, o registro deste fato.

<sup>4</sup> "O número de transistores em um chip aproximadamente dobrará a cada 24 meses". Esta previsão, feita em 1.965 por Gordon Moore, co-fundador da Intel, ficou conhecida como Lei de Moore

<sup>5</sup> "So how do you do this? Well, it turns out that it isn't so bad. On our side, we have Moore's Law" (tradução livre)



acessível de um modo racionalmente estruturado.

Depois de ver a demonstração do protótipo do mecanismo de busca, Bechtolsheim se convenceu de que estava diante de dois empreendedores de imenso potencial, com uma solução pronta que resolvia um problema realmente grande, do qual ele mesmo era uma das vítimas:

Eu fiquei muito empolgado com a possibilidade de permitir que qualquer pessoa pudesse encontrar qualquer informação, a qualquer tempo, através deste formato de busca, que era muito melhor do que as disponíveis à época. Então, eu realmente investi na empresa para resolver meu próprio problema, que era encontrar informações na Internet, algo que, em 1998, era realmente muito difícil de fazer. (KNIGGE, 2009)<sup>6</sup>

Havia um problema bem definido, uma solução que resolvia adequadamente aquele problema e dois empreendedores hábeis que demonstraram ter toda a capacidade necessária para seguir à frente de uma empresa de tecnologia. Apenas uma pergunta ainda faltava ser respondida: existia um modelo de negócio que tornasse os mecanismos de busca economicamente viáveis? Esta pergunta parece, hoje, quase retórica, mas lá, em 1998, nenhum dos sistemas de busca disponíveis gerava receita diretamente com buscas. Apesar da resistência demonstrada por Brin e Page quanto a estabelecer a propaganda como fonte de geração de receita, pois acreditavam que a publicidade poderia corromper os resultados, este parecia um caminho claro para Bechtolsheim (VISE; MALSEED, 2018).

Articular imensa capacidade computacional para alocar anúncios de modo altamente eficiente, mesmo que isso implique em efeitos colaterais perniciosos, como a vigilância contínua e a articulação de dados pessoais que geram efeitos discriminatórios, foi um resultado efetivo deste nada fortuito encontro de agosto de 1998.

Ao final, Bechtolsheim preencheu um cheque de cem mil dólares nominal a Google Inc., uma empresa que até aquele momento não havia sequer nascido. Com sua chancela, não foi tão difícil para Brin e Page levantarem um milhão de dólares com outros investidores, dentre eles Jeff Bezos, fundador da Amazon (ISAACSON, 2014), e darem origem ao que se tornaria um império totalmente baseado em dados.

### 2.1.1 Latifúndios computacionais

Para colocar em funcionamento a computação intensiva de dados como a imaginada por Brin e Page com seu sistema de busca, é necessário mais do que montar e colocar para funcionar uma grande quantidade de computadores. É preciso fazer com que todos trabalhem em harmonia, gerando a maior eficiência em processamento

<sup>6</sup> Texto original: "I got very excited about the potential of allowing anyone to find any information anytime through this much better form of search compared to what was available at the time. So I really invested in the company to solve my own problem which was how to find information on the internet which in 1998 was actually a very difficult thing to do"(tradução livre).

possível. A computação distribuída tem exatamente este objetivo: fazer com que computadores espalhados por uma rede possam trabalhar juntos para a execução de um conjunto de tarefas.

No final dos anos 1990 e início dos anos 2000, uma série de iniciativas intensificavam o desenvolvimento dos sistemas distribuídos. Em Berkeley, o professor Erick Brewer liderava uma delas, que culminou no lançamento, em 1996, da Inktomi, empresa que rivalizou com o Google, e acabou sendo escolhida por empresas como o Yahoo! como fornecedora de *engine* de busca. Há uma distância temporal razoável, é possível ver, na diferença de destinos de Inktomi e Google, os resultados das estratégias de disponibilização direta dos serviços de busca - financiados essencialmente por publicidade - e de comercialização da tecnologia, caminho pensado por Page e Brin, mas contestado por Bechtolsheim, para que outras empresas atendessem às necessidades de busca dos clientes finais.

Com o desenvolvimento dos sistemas distribuídos, o servidor, ou seja, o computador unitário, deixou de ser uma unidade de medida limitadora, desencadeando dois fenômenos importantes para o entendimento da forma como estruturas computacionais capazes de processar volumes massivos de informação funcionam.

Antes, porém, é importante esclarecer o conceito de sistemas distribuídos. Nestes sistemas,

a existência de múltiplos computadores autônomos é transparente (isto é, não visível) para o usuário. Ele pode teclar um comando para rodar um programa, e ele rodará. O sistema operacional escolhe o melhor processador, encontra e transporta todos os arquivos de entrada para aquele processador e coloca os resultados no local apropriado. Em outras palavras, o usuário de um sistema distribuído não está consciente de que existem múltiplos processadores; ele o vê como um único processador virtual.<sup>7</sup>(TANENBAUM, 1996)

O primeiro dos dois fenômenos desencadeados pelo desenvolvimento dos sistemas distribuídos relaciona-se com o fato de que capacidades computacionais não necessariamente coincidentes com uma máquina individual puderam começar a ser articuladas como uma única máquina, já que uma camada lógica adicional passou a *esconder* toda a complexidade de articulação de diversos dispositivos necessária para disponibilização de uma capacidade computacional superior. Além da alocação mais eficiente de capacidade computacional, a ideia de virtualização aliada ao aumento da disponibilidade de banda de conexão, permitiu a oferta de capacidade computacional como *utility*<sup>8</sup>. A SUN Microsystems, a mesma empresa fundada por Bechtolsheim, foi

<sup>7</sup> No original: "the existence of multiple autonomous computers is transparent (i.e., not visible) to the user. He can type a command to run a program, and it runs. It is up to the operating system to select the best processor, find and transport all the input files to the processor, and put the results into the appropriate place. In other words, the user of a distributed system is not aware that there are multiple processors; it looks like a virtual uniprocessor."(tradução livre)

<sup>8</sup> Neste ponto, optou-se pela manutenção do termo em inglês por não haver um equivalente direto da palavra, em português, para este sentido. *Utility*, neste contexto, refere-se a uma capacidade que

uma das primeiras empresas a oferecer capacidade computacional como *utility*. Sua oferta inicial, em 1996, era CPU-hora por 1 dólar. A promessa era ousada para a época. Na página da companhia que apresentava a oferta era possível ler o seguinte: "Você pode acessar o poder computacional que precisar, quando você precisar, sem nenhum custo escondido, sem obrigações contratuais de longo prazo e aumentar ou decrescer o uso conforme sua necessidade de demanda"<sup>9</sup> (CASHMORE, 2006).

O segundo fenômeno relevante, trazido pelo desenvolvimento dos sistemas distribuídos foi a otimização de estruturas computacionais para garantir a escalabilidade de processamento em operações que demandam poder computacional intensivo. Como relembra Erick Brewer, o fundador da Inktomi que atualmente é vice-presidente de infraestrutura do Google, ao falar de sua experiência com clusterização:

O trabalho original que eu fiz em clusters e que levaram à Inktomi antecede as máquinas virtuais - pelo menos a reencarnação moderna das máquinas virtuais. Como consequência disso - e isso também é verdade para o Google, que iniciou em 1998, aproximadamente tendo a mesma idade da versão moderna das máquinas virtuais - não havia nenhuma noção de máquinas virtuais para montagem dos serviços.

Você construía sobre o hardware bruto. Inktomi e também o Google, no início, acabaram usando essencialmente um modelo de processo Unix e fazendo tudo em termos de processo, executando muitos processos no mesmo pedaço de hardware. De fato, o Google não usou máquinas virtuais até começar a fazer algumas coisas corporativas nas quais queria executar coisas de terceiros. Toda a estrutura interna nunca usou VMs.<sup>10,11</sup>

Um *Cluster*, neste contexto, é uma espécie de sistema distribuído, que pode ser definido como um conjunto de computadores interconectados por uma rede de alta velocidade e que trabalham juntos para executar tarefas de computação intensiva ou que envolva uma quantidade massiva de dados e que não poderiam ser executados por um computador individual. São usados, principalmente, para garantir alta disponibilidade e balanceamento de carga, permitindo ainda a disponibilização de nós redundantes de forma a tornar o sistema tolerante a falhas (SADASHIV; KUMAR, 2011). De forma diversa do conceito de máquina virtual, que *esconde* a arquitetura original dando a sen-

---

pode ser oferecida ao mercado por demanda, da mesma forma como ocorre com o fornecimento de energia elétrica, por exemplo.

<sup>9</sup> Texto original: "You can access the computing power you need, when you need it, with no hidden costs, without a long-term contractual obligation, and increase or decrease your usage as your demand requires."(tradução deste menstrando)

<sup>10</sup> VM, neste caso, é a abreviação de *Virtual Machine*, em português, Máquina Virtual.

<sup>11</sup> Texto original: "The original work that I did on clusters that led to Inktomi predates virtual machines — at least the modern reincarnation of virtual machines. As a consequence of that — and this is true for Google too, which was started in 1998 and which is roughly the same age as the modern version of virtual machines— there was no notion of virtual machines for building services.

You built on the raw hardware. Inktomi and also early Google ended up using essentially a Unix process model and doing everything in terms of processes, running many processes on the same piece of hardware. In fact, Google didn't use virtual machines really at all until it started doing some corporate stuff where it wanted to run third-party things. But all the internal stuff never used VMs."(tradução livre)

sação de uma única máquina que pode ser de propósito geral, nos clusters, a estrutura computacional é organizada para otimizar atividades intensivas de processamento e tratamento de dados.

Pode ser difícil imaginar como estas estruturas se articulam. Principalmente, pode ser difícil ter ideia do tamanho que estes clusters podem tomar. Em um artigo para a IEEE Micro, três engenheiros do Google apresentaram a arquitetura de cluster do sistema de busca existente em 2003. Cada cluster, possuía 15 mil computadores, PCs de mercado, formando um "cluster computacional de alto nível a um preço baixo"<sup>12</sup>(BARROSO; DEAN; HÖLZLE, 2003)

Todo esse avanço dos sistemas distribuídos viabilizou não apenas a possibilidade de disponibilização de aplicações altamente intensivas de capacidade computacional e processamento massivo de dados, em escala verdadeiramente global, com o nível de resposta com os quais estamos atualmente acostumados, na casa dos décimos de segundo, mas também abriu a possibilidade para que empresas de todos os portes e até mesmo pessoas físicas pudessem disponibilizar produtos e serviços pela internet. A computação em nuvem passou a ser uma realidade.

Três características marcam a computação em nuvem: primeiro, a ilusão de disponibilidade de recuso computacional infinito, que pode ser alocado sob demanda; segundo a eliminação de um comprometimento contratual antecipado om uma capacidade específica previamente alocada, tendo em vista que é possível começar pequeno e aumentar a quantidade de recursos utilizados apenas quando houver necessidade e, terceiro, a possibilidade de pagar pelos recursos computacionais com base nas necessidades de curto prazo e libera-los (liberando, conseqüentemente, o contratante da obrigação de pagamento) quando não for mais útil. (ARMBRUST *et al.*, 2009)

A partir deste momento, do ponto de vista de quem aluga capacidade computacional em serviços de nuvem, a necessidade de adquirir equipamentos, espaço de banda de conexão em contratos de longo prazo e caras licenças de software de base, como sistemas operacionais, sistemas de bancos de dados etc, dá lugar à comodidade da compra do *acesso*. Um modelo de alocação de recursos que levou, por exemplo, Eric Ries, uma das principais vozes ligadas ao empreendedorismo e ao estilo de empreender das Startups, autor do *bestseller Lean Startup* (Startup Enxuta) a falar em locação (aluguel) dos meios de produção. E complementou, em uma entrevista disponível no site ATotalDisruption.com: "Karl Marx, eu acho que sua cabeça explodiria se nós pudéssemos contar para ele que hoje qualquer criança com um cartão de crédito pode alugar meios de produção por menos que um dia de trabalho"<sup>13</sup>(RIES, 2015).

Apesar de controverso, esse é um posicionamento compreensível, tendo em

<sup>12</sup> Texto original: "a high-end computing cluster at a low-end"(tradução livre)

<sup>13</sup> Transcrição do original da entrevista:"Karl Marx, I think his head would explode if we could tell him that today any kid with a credit card can rent the means of production for like less than a day's wages."(tradução livre)

vista que, na geração anterior de startups, como aconteceu com o Google, o dinheiro captado dos investidores era alocado na construção de infraestruturas de hardware, software e conectividade necessárias para disponibilização dos serviços. Agora, com a capacidade computacional disponibilizada como *utility*, as startups não precisavam mais fazer essa alocação de recursos, liberando o dinheiro captado para melhorar seus produtos e para aumentar a base de clientes. Errar também ficou mais barato. Os experimentos com soluções digitais poderiam ser feitos com pequena alocação de recursos computacionais, alugados sem a necessidade de se estabelecer obrigações contratuais de longo prazo. A ideia de *fast fail* (errar rápido), amplamente apregoada por Ries tinha o ambiente perfeito para crescer e se espalhar como um mantra.

Visto de outro prisma, a partir de quem disponibiliza estas infraestruturas, observa-se claramente uma ultra concentração de poder computacional nas mãos de um número muito pequeno de empresas. O mercado de Infraestrutura como Serviço (IaaS), a modalidade de serviços em nuvem em que o contratante aloca, diretamente, capacidade computacional, cresceu 31,3% ao se comparar os resultados de 2017 e 2018, saltando de US\$ 24,7 bilhões para US\$ 32,4 bilhões, sendo que 77% deste mercado concentra-se em apenas cinco empresas, Amazon (47,8%), Microsoft (15,5%), Alibaba (7,7%), Google (4,0%) e IBM (1,8%).

Não coincidentemente, os principais *players* desse mercado também oferecem serviços digitais, seja diretamente para os usuários finais, tanto pretensamente gratuitos como mediante remuneração, seja para empresas nas duas outras modalidades de computação em nuvem: Plataforma como Serviço (PaaS), onde há maior agregação de valor pela inclusão de novas camadas de software, e Software como Serviço (SaaS) onde há a disponibilização de serviços completos. Isso porque o *aluguel* de capacidade computacional vai muito além de uma nova forma de geração de receita.

Sua origem, nos moldes como a conhecemos hoje, não é a mesma daquela imaginada por empresas como a SUN Microsystems, mas foi construída a partir da necessidade de compartilhamento de dados entre diversos players de uma mesma cadeia produtiva.

A criação da Amazon Web Services (AWS) ilustra bem esse novo modelo de disponibilização de serviços. Em 2002, Tim O'Reilly, fundador da maior editora de livros de tecnologia dos Estados Unidos, que leva o seu nome, foi a Seattle, na sede da Amazon, para se encontrar com Jeff Bezos. Nesta reunião, O'Reilly sugeriu a Bezos, a criação de ferramentas online, baseadas em API, para que outras empresas pudessem utilizar os dados gerados pela Amazon a partir dos hábitos de navegação e compra dos seus usuários.

A maneira como O'Reilly disse ter explicado a ideia de disponibilização de serviços baseados em APIs demonstra o poder desse conceito e como o compartilhamento dos dados e a forma como este compartilhamento acontece gera um círculo virtuoso

que devolve resultados financeiros a quem disponibiliza estes serviços, que vão muito além daquilo que as empresas pagam para utilizá-los (O'REILLY, 2002):

Como todos os proprietários de sites com quem conversei, Jeff tinha duas perguntas. O que há nisso para mim? Como vou ganhar dinheiro? Minha resposta foi a seguinte:

1. Sites como Amazon e Google são aplicativos. E a Microsoft demonstrou repetidamente que uma estratégia de plataforma supera sempre uma estratégia de aplicativos. Depois que outras empresas criam um valor agregado que depende de você, você tem um tipo de bloqueio benigno da indústria, que é uma vantagem competitiva real. (...)
2. A inovação virá das APIs que suportam *conseqüências não intencionais*. Como Bill Joy gosta de dizer: "Nem todas as pessoas inteligentes trabalham para nós". Oferecer aos desenvolvedores um *playground* amplia sua equipe de desenvolvimento, trazendo novas idéias e recursos ao mesmo tempo em que cria sua marca e imagem.
3. Obviamente, existem oportunidades de receita. Como o Google demonstrou, você pode fornecer acesso limitado gratuitamente para permitir que os desenvolvedores brinquem, mas licenciar para uso em larga escala. Portanto, quando as pessoas o procuram com aplicações pesadas, você pode, então, descobrir o negócio. (...) E, claro, no caso da Amazon, há uma oportunidade de receita embutida para os negócios existentes. Aplicativos de terceiros baseados na Amazon levam as pessoas de volta à Amazon, onde elas compram produtos.
4. Dar algo de volta à indústria, enriquecer o solo da inovação para todos, é bom como a reciclagem, vai muito além dos benefícios diretos que você colhe. As empresas precisam pensar não apenas o que podem obter das novas tecnologias, mas como podem habilitar outras. Um mercado é como um ecossistema. Quanto mais vida existe, mais existe para todos. É nas monoculturas que você começa a ter problemas.<sup>14</sup>

Bezos ouviu O'Reilly e descobriu que sua equipe de desenvolvimento já tinha iniciativas de desenvolvimento de APIs. Ainda em 2002, a Amazon realizou sua primeira conferência para desenvolvedores e esta iniciativa ganhou o nome de Amazon Web Services (AWS). A esta ideia de disponibilização de serviços, Bezos agregou

<sup>14</sup> Texto original: "Like every web site owner I've talked to, Jeff had a couple of questions. What's in this for me? How will I make money? My answer was as follows: 1. Web sites like Amazon and Google are applications. And Microsoft has demonstrated over and over again that a platform strategy beats an applications strategy every time. Once you have other companies building added value that relies on you, you have a kind of benign industry lock in that's a real competitive advantage. (...) 2. Innovation will come from APIs that support *unintended consequences*. As Bill Joy likes to say, "All the smart people don't work for us." Giving developers a playground extends your development staff, bringing in new ideas and features at the same time as it builds your brand and image. 3. There obviously are revenue opportunities. As Google demonstrated, you can provide limited access for free to allow developers to play around, but do licensing for large scale use. So when people come to you with heavy duty applications, you can figure out the deal then. (...) And of course, in Amazon's case, there is a built-in revenue opportunity for the existing business. Third-party Amazon-based applications do lead people back to Amazon, where they buy products. 4. Giving something back to the industry, enriching the soil of innovation for everyone, is good like recycling is good, far beyond the direct benefits you reap. Companies need to think not just what they can get for themselves from new technologies, but how they can enable others. A marketplace is like an ecosystem. The more life there is, the more there is for everyone. It's in monocultures that you start to have problems."(tradução livre)

outra, a de que os desenvolvedores poderiam aumentar o grau de uso das plataformas da Amazon, se a eles fossem disponibilizados serviços elementares, como blocos que pudessem ser utilizados para qualquer finalidade. Assim nasceram o EC2 (Elastic Computer Cloud) e o S3 (Simple Storage Service), as duas bases das ofertas de serviços em nuvem da AWS (STONE, 2019).

A disponibilização de serviços fáceis de serem acessados e utilizados por desenvolvedores se aliou à ideia da computação como *utility*. O Próprio Bezos traçou um paralelo entre capacidade elétrica e a capacidade computacional, disponibilizada pelo AWS (STONE, 2019), maior operação de computação em nuvem do mundo, na atualidade, e detentora de quase metade do mercado global de IaaS:

Cem anos atrás, se você quisesse ter eletricidade, precisaria construir a sua própria pequena usina elétrica, e muitas fábricas faziam isso. Assim que a rede elétrica foi ligada, eles descartaram seu gerador elétrico e começaram a comprar energia da rede. Isso faz mais sentido. E é isso que está começando a acontecer com a infraestrutura computacional.

A disponibilização de capacidade computacional, juntamente com serviços digitais especializados que podem ser utilizados por outras empresas, também ajuda a atrair um grande volume de desenvolvedores, que passam a usar o ambiente computacional disponibilizado pela empresa e se acostumar, se familiarizar, a este ambiente. Isso facilita a expansão do uso, por esses desenvolvedores, de outros produtos da empresa fornecedora de serviços em nuvem, o que, em grande medida, impulsiona outros negócios da empresa, tanto voltados para o mercado empresarial quanto para atendimento direto do consumidor final. Esta vantagem competitiva, de ter um grande volume de desenvolvedores e startups utilizando suas plataformas de computação em nuvem, foi reconhecida por Erick Schmidt, então CEO do Google, ao comentar a liderança da Amazon neste segmento: “[é] uma vantagem significativa quando todas as empresas interessantes que estão crescendo rápido começam a ser desenvolvidas na sua plataforma” (STONE, 2019).

Um exemplo desta oferta cruzada de produtos é a relação existente entre Google e Uber. As capacidades de mapa e serviços de localização utilizados pela Uber são, em grande medida, prestados pelo Google, com sua plataforma Google Maps. Pela utilização destes serviços, a Uber pagou, pelo período de 1º de janeiro de 2016 a 31 de dezembro de 2018, o valor de US\$ 58 milhões. Uma fração do US\$ 631 milhões pagos a todas as subsidiárias da Alphabet (controlador do Google) para utilização de serviços de marketing e publicidade. Além disso, a Uber também utiliza serviços de nuvem do Google Cloud, juntamente com o AWS (NOVET, 2019).

Os serviços de localização e mapa estão no coração da oferta da Uber. O domínio desta tecnologia é estratégica para uma empresa que, em 12 meses (de setembro de 2017 a setembro de 2018) intermediou 5 bilhões de corridas de transporte individual. Uma vulnerabilidade deste tamanho, a dependência de outro fornecedor de tecnolo-

gia para tornar sua oferta viável, exigiu uma manifestação explícita da companhia no prospecto de abertura de ações da empresa (UBER TECHNOLOGIES, 2019).

Contamos com terceiros para fornecer software para nossos produtos e ofertas, incluindo o Google Maps para a função de mapeamento que é essencial para a funcionalidade de nossa plataforma. Não acreditamos que exista uma solução alternativa de mapeamento que possa fornecer a funcionalidade global necessária para oferecermos nossa plataforma em todos os mercados onde operamos. Não controlamos todas as funções de mapeamento empregadas por nossa plataforma ou pelos motoristas que usam a nossa plataforma e é possível que essas funções de mapeamento possam não ser confiáveis. Se esses terceiros deixarem de fornecer acesso a este software que nós e os nossos motoristas usamos ou caso não forneçam acesso a esse software nos termos que acreditamos serem atraentes ou razoáveis, ou não nos forneça a versão mais atual de tal software, podemos ser levados a procurar software compatível de outras fontes, que podem ser mais caras ou inferiores, ou podem não estar disponíveis, o que pode afetar adversamente nossos negócios.<sup>15</sup>

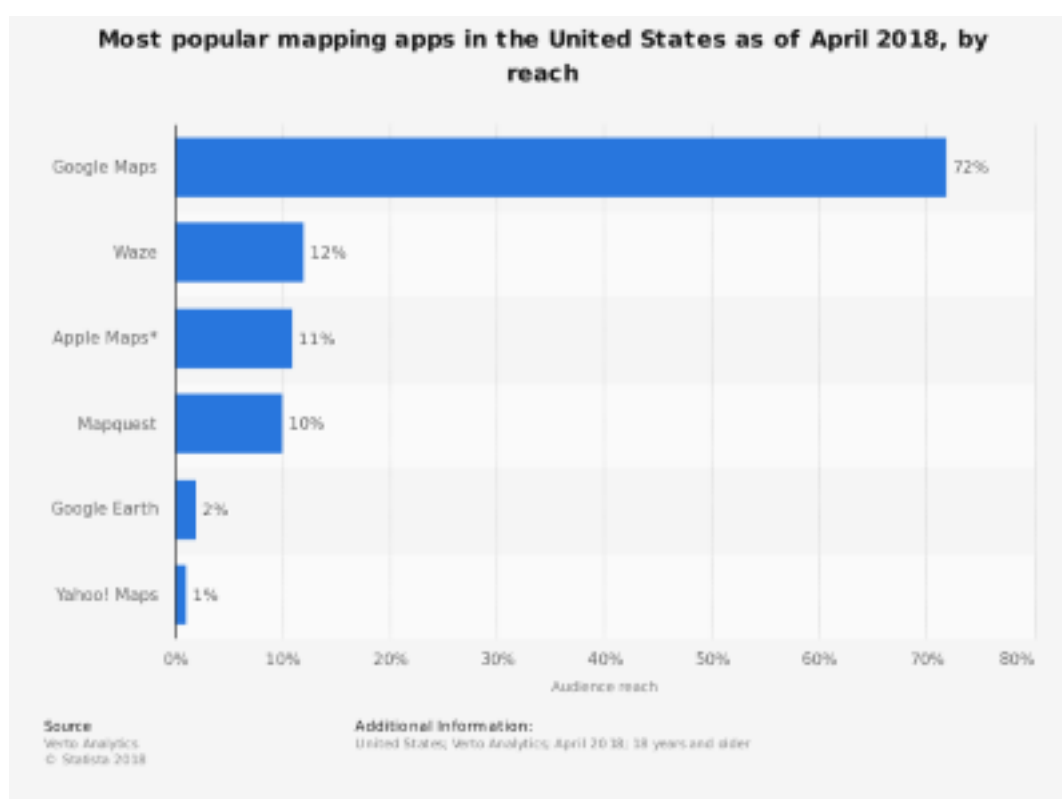
O Google, com seus produtos Google Maps, Waze e Google Earth domina mais de 85% do mercado de aplicações de mapa, como demonstra o gráfico do site Statista (VERTO ANALYTICS, 2019). É, claramente, um cenário de quase monopólio, que é alimentado com dados de tráfego e localização gerados não apenas por quem utiliza diretamente estes aplicativos, mas também por todos que utilizam - motoristas e passageiros - os principais serviços de transporte por aplicativo, tendo em vista que o Lyft, maior concorrente da Uber, também usa o Google Maps como seu fornecedor de solução de mapas e geolocalização (LYFT, 2019). Um quase monopólio, que alimenta um oligopólio que, por sua vez, retorna mais dados à empresa quase-monopolista, ajudando-a a tornar seus serviços ainda mais eficientes e consolidando sua posição quase-monopolista.

Essa armadilha de monopólios e oligopólios, que aumenta a capacidade de captura de dados pessoais e, conseqüentemente, de vigilância e perfilização por parte das empresas que disponibilizam serviços digitais, criando ameaças reais a Direitos Fundamentais, dificilmente é combatida por legislações de proteção aos dados pessoais como a LGPD, no Brasil, e a GDPR, na Europa. Uma abordagem aprofundada deste fenômeno será realizada no capítulo 3.

<sup>15</sup> Texto original: "We rely upon certain third parties to provide software for our products and offerings, including Google Maps for the mapping function that is critical to the functionality of our platform. We do not believe that an alternative mapping solution exists that can provide the global functionality that we require to offer our platform in all of the markets in which we operate. We do not control all mapping functions employed by our platform or Drivers using our platform, and it is possible that such mapping functions may not be reliable. If such third parties cease to provide access to the third-party software that we and Drivers use, do not provide access to such software on terms that we believe to be attractive or reasonable, or do not provide us with the most current version of such software, we may be required to seek comparable software from other sources, which may be more expensive or inferior, or may not be available at all, any of which would adversely affect our business."(tradução livre)



Figura 1 – Aplicativos de Mapas mais Populares nos Estados Unidos em Abril de 2018, por alcance.



Fonte: Statista.

Como no caso dos aplicativos de transporte, o modelo de compartilhamento atravessou os limites dos serviços puramente digitais e ganhou as ruas. Carros, para transporte de passageiros, quartos, casas e apartamentos, para aluguel por temporada, estruturas logísticas, para entregas rápidas, tudo passou a ser *compartilhado*. Os modelos de negócio criados pelas empresas que disponibilizam aplicações na Internet passaram, então, a ser adaptados a outras indústrias. Michael Porter, um dos autores mais prestigiados de todos os tempos na área de negócios, publicou dois artigos na Harvard Business Review, em 2014 e 2015, mostrando como os produtos inteligentes e conectados estão, respectivamente, transformando as companhias (PORTER; HEPPELMANN, 2014) e a competição (PORTER; HEPPELMANN, 2015). A transformação digital passou a ser um imperativo nas empresas.

A *economia do compartilhamento*, mais especificamente, é uma realidade visível. Uma reprodução ampliada de um modelo de negócios pensado originalmente para serviços digitais e expandido, à forma descrita por Porter, para muitas outras indústrias, com todas as suas virtudes de otimização, mas também carregando suas vicissitudes, como uma tendência fortemente monopolista e de concentração de propriedade, que reconfiguram mercados e mudam, para o bem e para o mal, estruturas sociais

relevantes, como as formas de organização do trabalho.

É a partir da compreensão deste intrincado contexto - onde menos de dez empresas concentram gigantesco poder computacional e o utilizam para disponibilizar serviços não remunerados diretamente pelos usuários, baseados no tratamento de dados pessoais, e, ao mesmo tempo, oferecem parte desta capacidade para que outras empresas possam criar novas soluções, remuneradas ou não, diretamente pelos usuários, mas que também fazem tratamento de dados pessoais, muitas vezes utilizando plataformas disponibilizadas por estes mesmos grandes conglomerados formados de poder computacional, alimentado-os com dados pessoais mesmo quando não são diretamente visíveis para os usuários e tornando seus modelos de segmentação, perfilação e predição de comportamentos mais eficientes - que devem ser pensadas as formas de regulação capazes de proteger os direitos da personalidade. Personalidade da qual os próprios dados pessoais fazem parte.

### 2.1.2 *Cookies, APIs e Open Source*

O Hypertext Transfer Protocol (HTTP), protocolo de comunicação que é a base Web, foi originalmente projetado de tal forma que cada requisição de um determinado cliente (feita por um navegador) era entendida como uma nova conexão pelo servidor acionado para atender a requisição. Assim, um servidor tratava uma nova conexão de forma completamente independente das anteriores, como se fosse a primeira, impedindo a identificação de estados do usuário no uso de uma aplicação online. Com essa característica, de não manter informações mínimas persistentes entre conexões com o servidor, era muito difícil implementar aplicações que exigem um fluxo contínuo de navegação onde o passo seguinte depende das decisões anteriormente tomadas pelo usuário como, por exemplo, implementar um carrinho de compras em um e-commerce. Em 1994, Lou Montulli, que trabalhava na Netscape<sup>16</sup>, escreveu a especificação original do que chamou de *cookie*. Com ele, um servidor, respondendo a uma requisição, pode enviar, na camada de protocolo e não na de conteúdo, algumas informações arbitrárias para o computador do cliente e armazená-las em pequenos arquivos. Qualquer tipo de informação pode ser enviada, como a identificação de um usuário, uma chave de banco de dados ou informações úteis para que o servidor saiba onde o usuário parou naquela conexão, de forma que a próxima consiga aproveitar essas informações. Estabelece-se, então, um contrato entre servidor e cliente, onde o servidor confia no cliente para salvar o status atual, de forma a poder resgatá-lo no próximo acesso (KRISTOL, 2001).

<sup>16</sup> Marc Andreessen desenvolveu, junto com Eric Bina, o Mosaic, um dos primeiros navegadores web e o primeiro a incorporar imagens. Em 1994, Andreessen juntou-se ao empreendedor em série Jim Clark e, juntos, fundaram a Netscape, que produziu uma versão comercial do Mosaic. (ISAACSON, 2014)

Com esse mecanismo de persistência de estado, passou a ser possível não apenas reaproveitar informações para reutilização no ciclo de navegação seguinte, mas também manter agrupados vários dados de um usuário mesmo antes de saber quem ele é. A navegação em um e-commerce é um bom exemplo. O usuário entra na loja e navega. Não tenta fazer uma compra, nem dá seus dados de identificação. Mas com os *cookies*, o servidor consegue rastrear todos os seus passos pelo site até que, em um determinado momento, ele decide fazer a compra. Identifica-se, portanto. Então, aquela aplicação não passa a conhecer o usuário a partir desse momento. Ela já o conhece desde a primeira vez que ele a acessou. Agora, ela apenas sabe o seu nome.

Um outro fenômeno, porém, torna essa possibilidade de rastreamento de comportamentos de navegação ainda mais eficiente. Uma determinada página web pode incorporar trechos de código que acionam *cookies* de terceiros, ou seja, permite que, a partir de uma página se inicie uma comunicação entre a máquina cliente e outros servidores, de forma quase imperceptível para o usuário. Imagine que aquele usuário do exemplo anterior tenha uma conta em algum serviço Google, como o GMail, por exemplo, e se conectou a ele a partir do seu computador ou *smartphone*. Muito possivelmente o site de e-commerce utiliza uma ferramenta de análise de navegação como, por exemplo, o Google Analytics. Se essa for a opção, a loja virtual usará *cookies* do Google para gerar as informações estatísticas de uso. Só que o Google sabe quem é o usuário, porque ele se logou em um dos seus serviços e os *cookies* destes serviços também passaram a rastreá-lo. Isso significa que a loja não conhecia o usuário desde o início, mas o Google, sim. É exatamente esse mecanismo de *cookies* acionado a partir de servidores (e serviços) externos às plataformas que possibilita a exposição de anúncios personalizados baseados no histórico de navegação do usuário, em uma estratégia designada por *retargeting*, que permite, por exemplo, que uma compra frustrada nas últimas etapas, em um e-commerce, passe a gerar anúncios específicos sobre aquele produto que quase foi adquirido, muitas vezes acompanhado de um desconto, nos sistemas de busca, nas redes sociais e nos diversos sites e portais servidos por redes de *display*.

Essa sensação de que a navegação está sendo vigiada, quando esses anúncios começam a aparecer, não é apenas uma sensação. *Cookies* de terceiros estão espalhados por toda parte. São usados indiscriminadamente, muitas vezes sem um juízo de valor adequado quanto à real necessidade de cada um deles. O próprio processo de reaproveitamento de código, entre projetos ou mesmo de códigos recebidos como parte de um *framework* de programação, pode facilitar a incorporação dos *cookies*. Um bom exemplo de como esses pequenos espiões estão infiltrados nas páginas mais diversas é o próprio site da Universidade Federal de Santa Catarina (UFSC). Em 15 de janeiro de 2020, foi realizada uma varredura, utilizando-se a ferramenta Cookiebot, em

cinco páginas acessíveis a partir do endereço principal da universidade ([www.ufsc.br](http://www.ufsc.br)). A ferramenta encontrou 14 *cookies* no total, sendo dois deles necessários para o bom funcionamento do site, utilizados para preservar a sessão do usuário enquanto navega, e mais onze *cookies* de marketing, todos ligados ao Google (9 do Youtube e 2 da Doubleclick). Um *cookie* não teve a categoria identificada pela ferramenta. Dois dos *cookies* de marketing são especialmente interessantes e valem destaque. O primeiro, da DoubleClick, possui a seguinte descrição de finalidade: “[u]sado pelo Google DoubleClick para registrar e reportar as ações dos usuários do website após visualizarem ou clicarem em um dos anúncios de publicidade, com o propósito de mensurar a eficácia de um anúncio e para apresentar anúncios direcionados ao usuário”<sup>17</sup>. O segundo, do Youtube, “registra um ID [identificador] único no dispositivo móvel para possibilitar o rastreamento baseada na localização geográfica por GPS”<sup>18</sup>. Fica, nesse ponto, a dúvida sobre a necessidade de utilização dos *cookies* de marketing no site institucional de uma universidade pública. Se foram incluídos como parte de uma estratégia de presença digital ou se foram colocados por padrão, a partir de alguma base de código pré-existente. Independente das respostas, esse exemplo demonstra como os *cookies*, que direcionam informações sobre navegação para grandes concentradores de dados pessoais, como o Google e o Facebook, estão espalhados por todos os lados, até mesmo onde menos se espera.

O relatório com os resultados completos é apresentando no Anexo A deste trabalho.

Outros mecanismos também são utilizados para rastreamento de navegação como os *web bugs*, pequenos gráficos, de 1 por 1 pixel, invisíveis aos usuários e que são utilizados para monitorar quem faz o acesso a uma página web ou a um e-mail (SMITH, 1999). Também podem entrar nesse rol, por exemplo, o armazenamento local do HTML5, os *Local Shared Objects* e as técnicas de *fingerprinting* (registro de impressão digital), esta última utilizada para identificar informações relativas aos dispositivos utilizados pelos usuários (ICO, 2019a).

A capacidade de, em um ponto da web ser possível iniciar uma operação de processamento de dados em outro ponto, a partir da inserção de um trecho de código em uma página ou em uma aplicação, não funciona apenas para *cookies*. A disponibilização de aplicações ou funcionalidades, por uma organização, para a comunidade de desenvolvedores é uma das bases do que ficou conhecida como Web 2.0. Esse rótulo, criado por Tim O’Reilly, vê a Web como uma plataforma, na mesma linha de raciocínio utilizada pelo próprio O’Reilly na sua conversa com Bezos, da Amazon, citada na Se-

<sup>17</sup> No original: “Used by Google DoubleClick to register and report the website user’s actions after viewing or clicking one of the advertiser’s ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.” (tradução livre)

<sup>18</sup> No original: “Registers a unique ID on mobile devices to enable tracking based on geographical GPS location.” (tradução livre)

ção 2.1.1. Para ele, a nova web tinha como grande referência o Google, em contraste com empresas dos ciclos tecnológicos anteriores, em especial as que nasceram junto com a web da primeira geração, como a própria Netscape (O'REILLY, 2007).

Ao fazer uma definição, em sua página na internet, em 2006, da Web 2.0, O'Reilly (2006) cita, como uma das suas regras: “em um ambiente de rede, APIs abertas e protocolos padrão vencerão, mas isso não significa que a ideia de vantagem competitiva desapareceu”<sup>19</sup>. Com o passar dos anos, observou-se que a capacidade de articular protocolos padrão e disponibilizar métodos de conexão para que a comunidade de desenvolvedores pudesse encurtar o tempo de desenvolvimento de suas soluções utilizando, para tanto, serviços providos por terceiros, tornou-se uma nova fonte de vantagem competitiva.

Assim, sobre a mesma estrutura da web original, desenvolvida essencialmente para que seres humanos tivessem acesso direto a informações, novas utilizações passaram a ser realizadas, onde a comunicação não se destinava mais a entregar conteúdo diretamente, mas a promover a integração entre aplicações. Novas formas de estruturação de dados foram criadas, como o Extensible Markup Language (XML), para facilitar a interoperabilidade. Assim, uma aplicação poderia trocar dados com outras de tal forma que, juntas, pudessem oferecer um serviço ao cliente final. A ideia de APIs abertas, que podem ser utilizadas e integradas por qualquer desenvolvedor, gratuitamente ou a preços atrativos, e as outras formas de integração entre aplicações, que genericamente podem ser chamadas de *embed codes*, criaram uma nova dinâmica no fluxo de dados, antes praticamente restrita a uma comunicação entre o navegador, operado por um ser humano, e um servidor que reagia a solicitações.

Agora, com as diversas possibilidades de integração, uma solicitação de usuário pode envolver dezenas de aplicações diferentes, disponibilizadas por diferentes fornecedores, a maioria invisíveis ao usuário. Os dados são compartilhados, com cada um desses *players*, para que executem não apenas frações do serviço a ser entregue, mas também para realizarem outras atividades, de análise e gerenciamento, por exemplo, ou até para viabilizarem a monetização da aplicação original, como no caso dos sistemas de exibição de anúncios.

Nesse ponto, vale retornar ao exemplo do Google Analytics. Para utilizá-lo, basta incluir algumas linhas de código nas páginas web de um determinado site<sup>20</sup>, para que a biblioteca do Google (*analytics.js*), com o algoritmo necessário para captura das informações, possa ser executada. Assim, as informações de navegação do usuário passam a ser transmitidas para o Google, que pode integrá-las a informações capturadas por outras fontes, centralizando-as em um perfil de usuário. Quanto mais donos

<sup>19</sup> No original: “in a network environment, open APIs and standard protocols win, but this doesn't mean that the idea of competitive advantage goes away” (tradução livre)

<sup>20</sup> O Google Analytics também pode ser utilizado para integração de dados originados a partir de aplicativos móveis.

de sites e aplicações utilizarem sua plataforma de análise de performance, mais dados são gerados e, com mais informações sobre os usuários, mais eficiente se torna a segmentação para a entrega de anúncios. Por isso, também neste ponto, oferecer gratuitamente a ferramenta de análise passa a fazer sentido. Na verdade, o dono do site ou aplicação paga pelo uso da plataforma de análise de desempenho com aquilo que não é dele, ou seja, os dados pessoais daqueles que acessam seus produtos, serviços ou conteúdos.

A integração entre aplicações também permite que grandes detentores de poder computacional possam desenvolver e distribuir aplicações que suportam outros negócios, até tornarem-se imprescindíveis em diversos mercados. A construção de oligopólios, como as plataformas de transporte individual, sobre uma plataforma tecnológica de mapas e geolocalização que praticamente monopoliza o mercado, como no caso do Google Maps, é um bom exemplo de como a integração de aplicações pode favorecer a concentração de mercado e, também, de dados pessoais nas mãos de poucas organizações.

Toda esta arquitetura formada por *cookies* e integração de aplicações torna possível a expansão dos pontos de captura de dados pessoais para fora dos domínios originais de um determinado *player*. Grandes concentradores de dados passam, então, a oferecer novos serviços para clientes de outros lados, do mercado de múltiplos lados, utilizando a mesma lógica da gratuidade, de modo a terem acesso às propriedades digitais destes clientes para, a partir delas, poderem capturar mais dados. A essa teia de conexões costurada a partir da inserção de pequenos códigos em sites e aplicativos dos outros, para obtenção de mais dados pessoais, dá-se o nome, neste trabalho, de capilaridade lógica, em contraposição à capilaridade física que será tratada na Seção 2.1.3.

Uma outra forma de expansão de domínio se dá pela disponibilização de aplicações *open source* e pela distribuição gratuita de software. Um exemplo claro desse modelo, que também pode ser caracterizado como uma estratégia de expansão da capilaridade lógica, é o navegador Google Chrome que, com essa forma de distribuição, alcançou uma posição dominante de mercado. Como o navegador é a ponta final das aplicações web, controlá-la permite estabelecer os novos padrões de comunicação, da mesma forma como fez a Netscape, no final do século passado, ao definir os padrões de *cookie*. Esse mesmo movimento será observado em breve, com a substituição dos padrões atuais por outros, em um movimento liderado pelo próprio Google, que será detalhado na Seção 4.1.1.

### 2.1.3 Transistores e sensores em todos os lugares

A vida não foi fácil para Joe Chip, mesmo enquanto ele tinha a convicção de que estava vivo. No dia em que conheceu Pat Conley, em seu apartamento, antes de

abrir a porta, ligou para o ramal do circuito de manutenção do prédio para solicitar o envio de um robô de limpeza. Seu pedido foi negado, pela “entidade homeostática” que o atendeu, alegando que uma agência de análise de crédito publicou um informativo classificando-o no status G quádruplo de crédito, um estágio considerado, pelos sistemas de análise de riscos do prédio, como uma anomalia que impedia qualquer tipo de disponibilização de serviços sem pagamento antecipado.

Depois de tomar um café, com Pat e G. G. Ashwood ainda esperando do lado de fora, estava preparado para recebê-los. Tentou abrir a porta e a porta lhe disse: “[c]inco centavos, por favor”. Joe força a maçaneta e interpela a porta dizendo que não tem obrigação de pagá-la. A porta, então, retruca: “[p]enso diferente. Olhe no contrato de compra que você assinou ao adquirir este condapto”. Incrédulo, foi até à gaveta da escrivaninha e pegou o contrato. Era verdade. A taxa de abertura e fechamento da porta era obrigatória, no que a porta debochou: “[d]escobriu que estou certa”. Desesperado, Joe vai até a cozinha e tira, da gaveta ao lado da pia, uma faca de aço inoxidável e, com ela, começa a desparafusar o ferrolho da porta que, logo após a queda do primeiro parafuso, o adverte: “[v]ou te processar” (DICK, 2015).

Em 1.969, quando a distopia psicodélica *Ubik*, escrita por Philip K. Dick, foi lançada, um diálogo como este era algo restrito aos livros de ficção científica. Vista a partir da ótica de um habitante da Terra, em 1.992, quando a história foi ambientada, pareceria insólito, apesar de não soar impossível em um futuro próximo. Hoje, possui ares de normalidade.

Milhões de pessoas conversam, em linguagem natural, com suas assistentes virtuais, como Alexa e Siri, disponibilizadas, respectivamente, por Amazon e Apple, obtendo respostas, em grande medida acuradas, a perguntas específicas e também realizando pequenas atividades, como comandar acionamento de luzes e dispositivos domésticos, selecionar e tocar músicas, realizar anotações na agenda de compromissos e fazer ligações. Apesar de, atualmente, as assistentes virtuais dependerem de uma ação direta do usuário, ou seja, necessitarem de um comando para executarem uma tarefa, em um futuro bem próximo estas aplicações poderão agir a partir do entendimento do contexto, sem a necessidade de um comando explícito. Dave Limp, Vice-Presidente Sênior de Dispositivos e Serviços da Amazon, explica como a nova geração da Alexa trabalha com decisões contextuais: “Se eu caminho em um quarto na minha casa, eu não preciso dizer ‘Acenda a luz na cozinha ou na sala de estar’. Depois de um tempo configurada, a Alexa, no quarto, *entende o contexto* e sabe ligar a luz naquele quarto. Eu posso dizer assistir ‘X, Y, Z no Netflix’ e ela sabe em qual quarto eu estou e qual TV deve ligar.”<sup>21</sup>

<sup>21</sup> No original: “If I walk into a room of my house, I don’t have to say, ‘Turn lights on in kitchen or living room,’”he explained. After a one-time setup, the Alexa in the room “understands context”and knows to turn the lights on in that room “I can say watch ‘X,Y,Z on Netflix’ and it knows what room I’m in”and what TV to turn on”(tradução livre).

Até mesmo a ameaça da porta, de processar Joe Chip já não soa insólita. Em 2017, o Parlamento Europeu aprovou uma resolução com disposições de Direito Civil sobre Robótica, que em suas recomendações relativas a responsabilidade, apresenta a possibilidade de criação de um estatuto jurídico específico para os robôs, de pessoa eletrônica, aplicável a casos em que haja decisões autônomas ou interações independentes destes equipamentos com terceiros (PARLAMENTO EUROPEU, 2017). Como a própria resolução estabelece a necessidade de um suporte físico mínimo, a porta poderia ser elegível ao status de robô, podendo caber-lhe, portanto, personalidade jurídica suficiente para reclamar em juízo eventuais danos causados por atos deliberados de vandalismo.

É inegável que a vigilância ambiental, até certo ponto autorizada pelos usuários, promovida por este tipo de equipamento, pode gerar riscos proeminentes à privacidade e outros direitos da personalidade impactados pelas atividades de tratamento de dados pessoais. Aqui, é impossível não voltar novamente ao romance de Philip K. Dick, que engarrafa em um spray uma substância, Ubik, que deve estar em tudo para que a vida se mantenha, da mesma forma como os planos de dados mantém a todos conectados. O caráter ubíquo da rede não se limita aos assistentes virtuais, que estão em nossas casas, mas também nos acompanham em nossos celulares e até nos pequenos fones sem fio, como é o caso do novo Echo Buds, da Amazon (EADICICCO, 2019). Onipresença e Onisciência ganham contornos ainda mais fortes com o avanço do que se convencionou chamar de Internet das Coisas (IoT).

Sob a ótica técnica, IoT pode ser conceituado como um "grupo de infraestruturas que interconectam objetos conectados e permitem seu gerenciamento, mineração de dados e o acesso aos dados que eles geram".<sup>22</sup> Já *objetos conectados* são definidos como

sensor(es) e/ou atuador(es)<sup>23</sup> que executam uma função específica e que podem se comunicar com outro equipamento. Fazem parte de uma infraestrutura que permite o transporte, armazenamento, processamento e acesso aos dados gerados por usuários ou outros sistemas.<sup>24</sup> (DORSEMAINE *et al.*, 2015)

A utilização de sensores e atuadores não é nova. A grande mudança trazida pela IoT, além da miniaturização destes dispositivos que, em grande medida, está ligada à capacidade de concentração de um imenso número de transistores em pequenos espaços (mais um efeito explícito da Lei de Moore), diz respeito à possibilidade de, por

<sup>22</sup> No original: "Group of infrastructures interconnecting connected objects and allowing their management, data mining and the access to the data they generate."(tradução livre)

<sup>23</sup> Um atuador é um componente de um sistema responsável por movimentar ou controlar um mecanismo ou outra parte desse sistema. (SEABRA, 2016)

<sup>24</sup> Texto original: "Sensor(s) and/or actuator(s) carrying out a specific function and that are able to communicate with other equipment. It is part of an infrastructure allowing the transport, storage, processing and access to the generated data by users or other systems."(tradução livre)



um lado, integrar os dados coletados pelos sensores a sistemas de processamento e mineração de dados, conectando-os com outras bases, e de outro, executar ações locais, via atuadores, a partir dos dados processados remotamente.

A arquitetura de infraestruturas de IoT, portanto, pode ser dividida em quatro camadas (DORSEMAINE *et al.*, 2015) e (LI; XU; ZHAO, 2015):

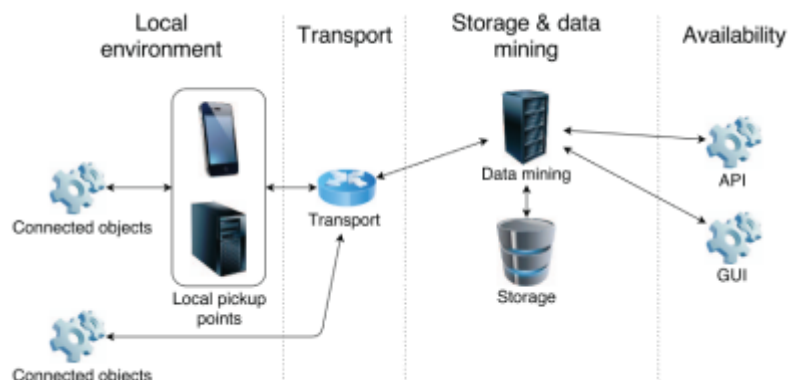
- a. **Camada ambiental ou camada de detecção**, onde estão efetivamente posicionados os sensores e atuadores, capazes de sentir o *status* das coisas e podem atuar diretamente no ambiente, além de outros equipamentos que podem atuar como concentradores locais de dados (*local pickup points*).
- b. **Camada de transporte ou de rede**, correspondente à estrutura de rede que suporta a conexão (com ou sem fio) dos dispositivos e a comunicação com os servidores.
- c. **Camada de armazenamento e *data mining* ou camada de serviço**, responsável pelo processamento e armazenamento dos dados, geralmente disponibilizada em uma infraestrutura de nuvem. Tem como função criar e gerenciar os serviços requeridos pelos usuários e aplicações.
- d. **Camada de disponibilização ou de interface**, onde os usuários e outros sistemas podem acessar os dados e estabelecer novas rotinas de processamento, utilizando interfaces, computacionais (via APIs, essencialmente) ou gráficas, também conhecidas como Interface Gráfica do Usuário (GUI), o que permite inclusive a interação direta com a camada ambiental.

Importante observar que apenas a primeira camada (ambiental ou de detecção) é exclusivamente caracterizável como IoT, sendo as outras estruturas pré-existentes (DORSEMAINE *et al.*, 2015). Isso fica bastante claro no gráfico que resume a infraestrutura de IoT.

À capilaridade lógica, decorrente da utilização de *cookies*, *embed codes* e APIs, agrega-se, com IoT, uma capilaridade física, capaz de perceber, agir e reagir a partir de dados captados localmente e processados remotamente, em imensas infraestruturas computacionais que, como já demonstrado anteriormente, são controladas por pouquíssimas companhias. Para se ter uma ideia desta imensa vascularidade de sensores e atuadores, segundo a empresa de pesquisas Gartner, em 2.020, estarão ativos mais de 20,4 bilhões de *coisas* conectadas, contra 6,4 bilhões em 2.016. Já para 2.021 este número deve saltar para 25 bilhões de pontos (WALLIN, 2019), com os gastos relacionados a IoT alcançando a marca de 1,2 trilhão de dólares, em 2022 (IDC, 2018).

A capilaridade física traz consigo um grande desafio. Como as camadas de detecção estão geograficamente espalhadas, elas tendem a ser controladas por um imenso número de organizações e entidades, na maioria das vezes as mesmas que

Figura 2 – Arquitetura de infraestrutura IoT.



Fonte: (DORSEMAINE *et al.*, 2015)

detêm a posse ou a propriedade dos locais onde esta camada está instalada. Uma atuação isolada, ou seja, o processamento dos dados captados pelas estruturas de IoT de uma única organização, limita o efeito de rede no processamento destes dados. Pode ser interessante, por exemplo, para uma rede varejista integrar dados sobre o número de visitantes das suas lojas, capturados por sensores de contagem de pessoas, por exemplo, com um *bureau de dados* para comparação do seu volume visitas com o volume médio consolidado do seu segmento.

Com o volume imenso de dados a serem “trocados” ou “transferidos” entre organizações e a assimetria de valor entre as diversas categorias de dados capturados pelas infraestruturas de IoT, tendo em vista que há dados mais valiosos, do ponto de vista de negócio, do que outros, surge a necessidade de estabelecer um mecanismo de mensuração de valor e viabilização de trocas mais eficiente. É preciso, também, resolver um outro problema: as infraestruturas IoT também podem ser utilizadas para a realização de transações que vão muito além da troca de dados, transações estas que tendem a ocorrer de forma muito intensa, envolvendo pequenos valores, conhecidas como microtransações.

Em 2015, David Sonstebo, Sergey Ivancheglo, Dominik Schieer e Sergey Popov<sup>25</sup> trabalharam juntos para criar uma criptomoeda que resolvesse esses problemas (ALVES FILHO, 2018). Juntos, criaram uma nova implementação de *distributed ledger*<sup>26</sup>, diferente do *blockchain*, base do *bitcoin*, primeira criptomoeda efetivamente implementada, pois não se estrutura em uma cadeia de blocos, mas em um emaranhado de nós, daí o nome *tangle* para a *distributed ledger* que suporta a IOTA, a criptomoeda especificamente desenvolvida para a indústria de IoT.

<sup>25</sup> O matemático russo Serguei Popov é professor do Instituto de Matemática, Estatística e Computação Científica (Imecc) da Universidade Estadual de Campinas - UNICAMP

<sup>26</sup> Literalmente, "livro-razão distribuído". Pode-se considerar *distributed ledger* como um gênero de tecnologia de registro de dados da qual fazem parte o *blockchain* e o *tangle*.

O desenvolvimento da IOTA possuía um objetivo claro: reduzir o custo de transação e viabilizar as microtransações. Segundo Sergey Popov, um dos criadores da criptomoeda, em 2018, a soma total das taxas pagas para viabilizar as transações em bitcoin chegavam a US\$ 100 mil a cada 10 minutos (ALVES FILHO, 2018). Diferente do bitcoin, onde existe a figura dos mineradores, detentores de grande capacidade computacional e responsáveis pela criação dos blocos onde as transações são registradas e que, por esse trabalho de *mineração*, são remunerados, com a IOTA essa figura desaparece, levando a zero a taxa paga para viabilização da transação.

Apesar do escopo alargado de categorias de transações viabilizadas pela IOTA, não se pode negar que a disponibilização de uma estrutura capaz de viabilizar a compra e venda de dados ocupa um papel central no seu modelo. Em 2017, a IOTA Foundation lançou seu Data Marketplace (DMP), justamente com o objetivo de facilitar o fluxo dos dados gerados por IoT. A definição do DMP IOTA, em sua página de lançamento, ilustra bem o contexto desta plataforma:

Os Data Marketplaces surgem como um meio para trocar dados, monetizar fluxos de dados e fornecer a base de novos modelos de negócios "inteligentes".

Nós nos referimos a essa nova onda de criação de valor, para a Internet de Tudo [*Internet of Everything*], como a "Economia das Coisas" ou a economia de máquina a máquina (M2M). Esse cenário de oportunidades para a sociedade e os negócios pode parecer futurista para alguns, mas é o foco de um número crescente de organizações em todos os setores. Conscientes da enorme oportunidade e de sua natureza transformadora - e potencialmente disruptiva -, acreditamos que a melhor abordagem para organizações e indivíduos que pensam a frente é explorar essas oportunidades de modo aberto, juntos <sup>27</sup> (HARBOR, 2019).

Obviamente, o escopo da Internet das Coisas vai muito além dos dados pessoais. Dentre outras aplicações, esta é uma peça chave no que se convencionou chamar de Indústria 4.0, com grande impacto em diversas cadeias produtivas, desde o agronegócio até a indústria aeroespacial. Por outro lado, abre-se uma forma nova de colocar em comércio os dados pessoais, inclusive substituindo o método de disponibilização destes dados em troca do acesso a serviços pretensamente gratuitos, obscuro por natureza, por um sistema de microtransações que balanceie disponibilização de dados e acesso, em um ambiente transacional mais transparente, como sugere a própria IOTA Foundation (IOTA FOUNDATION, s.d.).

Mas esta visão de maior *accountability*, que permite um controle mais preciso dos titulares sobre o fluxo de seus dados pessoais, não é única. Microtransações base-

<sup>27</sup> Data marketplaces emerge as a means to exchange data, monetize data streams and provide the basis of new "smart" business models. We refer to this new wave of value creation, for the Internet of Everything, as the "Economy of Things" or the machine-to-machine (M2M) economy. This opportunity landscape for society and business may sound futuristic to some, but it is the focus of a growing number of organizations across industries. Conscious of the massive opportunity and its transformative — and potentially disruptive — nature, we believe that the best approach for forward-leaning organizations and individuals is to explore these opportunities openly, together.

adas em IOTA também podem suportar a comercialização de dados entre empresas, em transações absolutamente invisíveis aos titulares, e, em muitos casos, dificilmente detectáveis por autoridades ou organizações de controle, pela própria natureza dos dados trocados que, muitas vezes, estão diretamente associados a uma coisa (equipamento) e são apenas indiretamente associáveis a uma pessoa natural.

Esta preocupação já foi externada, inclusive, pelo Article 29 Working Group, na dicção portuguesa Grupo de Trabalho do Artigo 29.º (WP29), em um parecer sobre IoT e seus impactos à privacidade e proteção de dados:

De modo geral, a interação entre objetos, entre objetos e dispositivos de indivíduos, entre indivíduos e outros objetos e entre objetos e sistemas de back-end resultará na geração de fluxos de dados que dificilmente podem ser gerenciados com as ferramentas clássicas usadas para garantir a adequada proteção dos interesses e direitos dos titulares de dados. Por exemplo, diferente de outros tipos de conteúdo, os dados enviados por IoT podem não ser adequadamente revisados pelo titular dos dados antes da publicação, o que inevitavelmente gera um risco de falta de controle e exposição excessiva ao usuário. Além disso, a comunicação entre objetos pode ser acionada, por padrão, de forma automática, sem que o indivíduo esteja ciente disso. Na ausência da possibilidade de controlar efetivamente como os objetos interagem ou de poder definir fronteiras virtuais definindo zonas ativas ou não ativas para coisas específicas, será extraordinariamente difícil controlar o fluxo de dados gerado. Será ainda mais difícil controlar o seu uso subsequente e, assim, evitar potenciais usos imperceptíveis. Essa questão de falta de controle, que também diz respeito a outros desenvolvimentos técnicos, como computação em nuvem ou big data, é ainda mais desafiadora quando se pensa que essas diferentes tecnologias emergentes podem ser usadas em conjunto<sup>28</sup> (WP29 - ARTICLE 29 DATA PROTECTION WORKING PARTY, 2014).

Em uma realidade onde os métodos tradicionais não são capazes de salvaguardar os direitos e liberdades individuais no tratamento de dados pessoais, novas formas de proteção passam a ser necessárias. Neste sentido, um olhar sobre IoT ajuda a entender a necessidade de uma atuação conjunta, quase simbiótica, entre os padrões regulatórios, estabelecidos no âmbito do Direito, e métodos computacionais que precisam ser desenvolvidos para garantir que o fluxo de dados ocorra dentro dos padrões estabelecidos pela regulação. É o caso, por exemplo, do uso da técnica de *data pro-*

<sup>28</sup> Texto original: "More generally, interaction between objects, between objects and individuals' devices, between individuals and other objects, and between objects and back-end systems will result in the generation of data flows that can hardly be managed with the classical tools used to ensure the adequate protection of the data subjects' interests and rights. For instance, unlike other types of content, IoT-pushed data may not be adequately reviewable by the data subject prior to publication, which undeniably generates a risk of lack of control and excessive self-exposure for the user. Also, communication between objects can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep. This issue of lack of control, which also concerns other technical developments like cloud computing or big data, is even more challenging when one thinks that these different emerging technologies can be used in combination."(tradução livre)

*venance*, ou proveniência de dados, para auditoria de conformidade de privacidade e proteção de dados em IoT.

Proveniência, neste contexto, pode ser entendido como

um registro da origem e das transformações aplicadas aos dados em um sistema. A proveniência visa responder às seguintes perguntas: De onde vêm os dados? Quem manipulou os dados? Quais transformações foram aplicadas? Os dados de proveniência podem ser representados como um grafo acíclico direcionado que descreve as relações entre os elementos que compõem um sistema (itens de dados, etapas de processamento, usuários, informações contextuais etc.). Esses elementos se enquadram em três categorias: entidades (itens de dados), atividades (transformações aplicadas aos dados) e agentes (pessoas no sentido jurídico)<sup>29</sup> (PASQUIER; SINGH *et al.*, 2018).

Assim, os requisitos regulatórios e dos usuários podem representar o *comportamento esperado do sistema*, os mecanismos técnicos de execução (*enforcement*) representam as *ações permitidas*, enquanto a proveniência de dados representa o *comportamento atual do sistema*. Dessa forma, a partir da análise de proveniência é possível identificar se a intenção do regulador está sendo capturada pelos mecanismos de *enforcement* e eventuais discrepâncias entre o comportamento esperado e o comportamento atual podem ser reportadas, permitindo a correção do mecanismo de *enforcement* (PASQUIER; SINGH *et al.*, 2018).

A proveniência também atua como um método de registro de evidências, que facilita os processos de auditoria, aumentando o grau de transparência e facilitando a prestação de contas (*accountability*), dois aspectos fundamentais regulados pelas legislações de proteção de dados, sendo alçados ao status de princípios tanto na LGPD brasileira quanto no GDPR europeu.

A construção de sistemas auditáveis e transparentes, em especial com a utilização da proveniência de dados e suas aplicações em cibersegurança e proteção de dados, tornou-se um grande desafio de engenharia de software, além disso, a *accountability by design* deve firmar-se como o objetivo central a ser alcançado pelas plataformas de IoT (PASQUIER; EYERS; BACON, 2019), o que só se tornará realidade com o alinhamento do arcabouço regulatório e das novas técnicas computacionais capazes de viabilizar os princípios da transparência e da prestação de contas.

Além do entendimento da necessidade de uma maior coordenação entre aspectos legais e computacionais para o aumento do nível de proteção dos direitos e garantias individuais nas atividades de tratamento de dados pessoais, avaliar os impactos da Internet das Coisas sobre a privacidade e a proteção de dados, decorrente

<sup>29</sup> Texto original: "a record of the origin of and transformations applied to data within a system. Provenance aims to answer the following questions: Where do data come from? Who manipulated the data? What transformations were applied? Provenance data can be represented as a directed acyclic graph describing the relationships among elements composing a system (data items, processing steps, users, contextual information etc.). These elements fall into three categories: entities (i.e. data items), activities (i.e. transformations applied to data) and agents (i.e. persons in the legal sense)." (tradução livre)

do aumento da vigilância promovida pela possibilidade de controle de dispositivos geograficamente dispersos e da utilização de grandes volumes de dados que podem ser integrados com outras fontes e processados de modo a limitar ou restringir direitos e liberdades, é fundamental para entender o contexto e o avanço dos riscos inerentes à adoção em alta escala desta tecnologia.

Outros dois motivos, menos óbvios, reforçam a necessidade de se abordar IoT no âmbito da privacidade e proteção dos dados pessoais: primeiro, a análise dos mecanismos que viabilizam as trocas de dados, monetizando seus fluxos, ajuda a compreender que novas formas de valoração e transação de dados pessoais já estão em curso e podem ser extrapoladas para outras relações, não diretamente associadas a IoT; segundo, o seu crescimento exponencial alinha a capilaridade física, aumentando brutalmente a massa de dados disponíveis para processamento, à capilaridade lógica, responsável por disponibilizar essa grande massa de dados, diretamente ou já pré-processada, para um imenso número de empresas, via APIs, permitindo novas atividades de processamento baseadas em dados pessoais e criando um ambiente ainda mais complexo, fundado em grande poder computacional e na capacidade de promover integrações de dados e serviços entre diversos *players*.

## 2.2 UM ALVO SEMPRE NA MIRA

Não foi a Internet quem inventou os modelos de negócio de remuneração indireta, onde o usuário final paga por serviços pretensamente gratuitos com a alocação do seu tempo. Essa é forma clássica dos meios de comunicação *broadcast*, essencialmente o rádio e a TV, fazerem dinheiro. Na verdade, as plataformas digitais adotam modelos de negócios complexos, capazes de fazer relações baseadas em remuneração direta parecerem situações de remuneração indireta, como será evidenciado na Seção 4.2.2.1

Apesar do rádio inaugurar seu uso massivo, foi na TV que este modelo encontrou o terreno mais fértil. O monopólio da visão. O ápice de um modo de construção de significado fundado em um único sentido, legado da arte renascentista e intensificado pelo surgimento da imprensa, a primeira linha de montagem criada pelo homem, que inaugurou a produção em massa (MCLUHAN; FIORE, 2011).

Mas ao contrário do que sonhou McLuhan, os meios eletrônicos não libertaram as pessoas do jugo da visão. Não ampliaram seus horizontes sensoriais. Agora é possível prender-se em diversas telas distintas sem perder o contexto. Uma mesma experiência se replica e continua em diversas telas. Além disso, agora, carregamos conosco, quase vinte e quatro horas por dia, uma tela individual, cuja dominância sobre as ações dos indivíduos pode causar, inclusive, mudanças posturais permanentes. Se McLuhan, que cunhou a expressão *aldeia global*, vivesse hoje, possivelmente veria uma relação entre o aumento no deficit sensorial e a postura curvada característica

daqueles que utilizam intensivamente o celular.

A grande diferença que marca os negócios financiados por publicidade, na Internet, daqueles implementados em outras mídias, está na capacidade de captura total do tempo, não apenas do tempo de atenção, mas do maior número possível de atividades de vida daquele que, em algum momento, será o alvo escolhido de uma ação publicitária ultrassegmentada. Assim, ao fixar uma estratégia de dominação do tempo dos usuários, os serviços digitais gratuitos, de um lado, criam novas oportunidades de apresentação de anúncios e, de outro, tentam inserir mecanismos de capturas de dados pessoais em circunstâncias onde as pessoas não estão utilizando diretamente os produtos destes fornecedores.

Andy Bechtolsheim, o primeiro investidor-anjo do Google, ao referir-se à empresa de Brin e Page, resumiu, muito bem esta estratégia, ainda em 2009, em uma entrevista para o Deutsche Welle (KNIGGE, 2009):

O Google está basicamente no negócio de publicidade e, é claro, existem muitas maneiras de fazer dinheiro com publicidade e a questão principal, claro, é conseguir que o maior número possível de pessoas veja seus anúncios. Portanto, a expansão na qual o Google está trabalhando com o Android, nos telefones celulares, e muitos de seus outros novos aplicativos tem como objetivo alcançar ainda mais atenção dos clientes e eu acho que a empresa está fazendo progresso em muitos desses aplicativos. Todo mundo usa o Google Maps e o Google Earth é muito bom e, de certa forma, não fica claro como, no primeiro dia, esses aplicativos fazem dinheiro, mas, como as pessoas usam esses aplicativos e eles também são implantadas em outros sites, eles ganham cada vez mais audiência. No final, a publicidade precisa da maior circulação, do maior número de pessoas que visualizam seus anúncios e é nisso que o Google está trabalhando.<sup>30</sup>

Essa captura total do tempo, feita diretamente ou por meio de outros serviços que utilizam plataformas concentradoras de dados pessoais, permite o surgimento de uma economia da vigilância. Para chegar a esse conceito, é necessário voltar os olhos para um outro fenômeno, que pretensamente conecta interesses comuns, criando um ambiente de ganhos mútuos para todos os participantes, que neste trabalho será chamado de *economia do encontro*.

### 2.2.1 A economia do encontro

Hal R. Varian, economista chefe do Google, entrou na companhia em 2002, como consultor, a convite do CEO Eric Schmidt. Seu interesse pela construção de

<sup>30</sup> Texto original: "Google is basically in the business of advertising and there are of course many ways to collect advertising dollars and the key issue of course is to get as many people to see your ads as possible. So the expansion that Google is working on the Android, the mobile phones, and many of these other new applications is all to achieve yet more customer traction and I think the company made a lot of progress in many of these applications. Everybody uses Google Maps and Google Earth is very nice and in some ways it isn't quite clear how this makes money on day one, but as people use these applications and they get deployed in other websites as well, they did get more and more of an audience. So in the end advertising needs the biggest circulation, the biggest number of people looking at their ads and this is what Google is working on."(tradução livre).

modelos capazes de explicar o comportamento social nasceu, aos 12 anos, quando leu a série *Fundação*, de Isaac Assimov, e se encantou por Hari Seldon (LEVY, 2012), personagem que estruturou a psico-história, definida por Gaal Dornick, biógrafo de Seldon, conforme descrito na 116ª edição da Enciclopédia Galáctica, publicada em 1.020 E.F., como “o ramo da matemática que trata das reações dos conglomerados humanos a estímulos sociais e econômicos fixos” (ASIMOV, 2009). Com uma sólida produção acadêmica, Varian é professor emérito da Universidade da Califórnia, Berkeley, em três departamentos: economia, negócios e gestão da informação (VARIAN, s.d.) e o responsável pela fundamentação econômica do sistema de leilões de anúncio do Google.

Em 2009, Varian publicou um vídeo, no Youtube (VARIAN, 2009), explicando o modo de funcionamento do sistema de leilão de anúncios do Google. De início, esclarece que o objetivo é conciliar os interesses de três partes: o anunciante, o usuário e o próprio Google. Os três participantes possuem motivações distintas: os anunciantes querem que o seu público clique no seus anúncios, os usuários querem ter acesso a conteúdo relevante e o Google quer entregar uma experiência boa para anunciantes e usuários.

Com um exemplo bastante simples, com três posições de anúncios e quatro anunciantes licitantes competindo para ocupar as três posições, primeiro demonstra um ganho real para o anunciante, já que o preço pago pelo anúncio, caso o anunciante venha a ocupar uma das posições, não será o lance efetivamente dado, mas “a quantia mínima necessária para manter a posição” (VARIAN, 2009), ou seja, o valor pago é necessariamente menor do que o valor do lance.

Em seguida, passa a explicar os impactos da relevância dos anúncios, como forma de contemplar os interesses dos usuários no processo de leilão. Para isso, apresenta o índice de qualidade do anúncio, que é composto por três elementos: taxa de cliques (CTR, Click-Through), o mais importante deles, resultado da divisão do número de cliques em um determinado anúncio pelo número total de visualizações; a relevância, um índice calculado pelo Google a partir da correlação do anúncio com a palavra-chave buscada pelo usuário, dentro do contexto da linha de busca, e “comprada” pelo anunciante; e, por último, a qualidade da página de destino.

O passo seguinte é indicar a ordem de apresentação dos anúncios, resultado da multiplicação entre o valor do lance e o índice de qualidade. Segue a explicação, indicando a fórmula do custo do clique (CPC) para uma determinada posição:

$$p_1 = \frac{b_2 Q_2}{Q_1} \quad (1)$$

onde  $p_1$  é o valor efetivamente pago pelo anunciante,  $b_2$  é o lance do anúncio classificado imediatamente depois, e  $Q_1$  e  $Q_2$  são os índices de qualidade dos dois anúncios.

E finaliza o vídeo mostrando o impacto do aumento da qualidade do anúncio



no seu preço final, demonstrando que um aumento da qualidade significa, necessariamente, uma diminuição do preço, já que a qualidade do anúncio (Q1) aparece como divisor na fórmula de definição do preço .

Por trás desta sistema eficaz de conexão de interesses, existe um *framework* teórico bastante complexo, que une economia e ciência da computação, incorporando o conceito econômico de incentivos ao design de algoritmos: o Projeto Algorítmico de Mecanismos ou *Algorithmic Mechanism Design*. Segundo Flávio Keidi Miyazawa, um "mecanismo é um processo algorítmico que escolhe uma solução social baseado nas preferências dos jogadores. Para isso, o mecanismo deve ter regras de funcionamento que incentivem os jogadores a declarar informações verdadeiras para que a escolha social seja feita adequadamente"(MIYAZAWA, 2010). Visto de outro ângulo, como explica o próprio Varian (VARIAN, 2008):

projeto de mecanismo é, em certo sentido, o inverso da teoria dos jogos: na teoria dos jogos, são dadas as regras de um jogo e o objetivo é prever o resultado; no projeto de mecanismo, é dado um conjunto de resultados esperados e o objetivo é criar um jogo capaz de alcançá-los<sup>31</sup>

Neste ponto, quando se trata de leilões de anúncios, não se pode perder de vista que "o conjunto de resultados esperados" refere-se à alocação eficiente de *slots*, ou seja, espaços nas telas dos usuários, gerando bons resultados de conversão para o anunciante e o maior volume de receita, no resultado consolidado do conjunto de leilões, para o provedor da plataforma.

Utilizados, inicialmente, em sistemas de busca, os sistemas de leilão em tempo real, para distribuição de anúncios, são aplicados, hoje, em cenários mais complexos do que o originalmente experimentado nas buscas, com destaque para a alocação dos espaços para anúncios em redes sociais, como o Facebook. O Prof. Tim Roughgarden explica as principais diferenças:

como os anúncios no Facebook diferem dos leilões básicos de busca patrocinada nos quais focamos até agora? Existem muitas respostas para essa pergunta. Por exemplo, determinar quais anúncios são "relevantes" em um leilão de busca patrocinada é amplamente determinado pela consulta de pesquisa do usuário, enquanto o Facebook deve usar outras informações para essa finalidade (como amigos de um usuário, atividade recente etc.). Além disso, os anúncios competem mais diretamente com os resultados orgânicos no Facebook (por meio de seu feed de notícias) do que em um leilão de busca patrocinada. Da mesma forma, espaços dedicados a anúncios são espaços retirados de outros tipos de conteúdo que o Facebook pode querer mostrar, como recomendações de amigos. Outra diferença é que os anúncios do Facebook têm tamanhos e formatos diferentes, em vez de apenas serem links patrocinados, cada um ocupando um único espaço. Por fim, o Facebook

<sup>31</sup> Texto original: "Mechanism design is, in a sense, the inverse of game theory: in game theory, one is given the rules of a game and the goal is to predict the outcome; in mechanism design, one is given a set of desired outcomes and the goal is to design a game that will achieve them."(tradução livre)

permite que os anunciantes ofereçam não apenas cliques, mas também muitos outros eventos (por exemplo, curtidas ou downloads de um aplicativo).<sup>32</sup> (ROUGHGARDEN, 2016).

Roughgarden também destaca a necessidade de imenso poder computacional para promover leilões, em tempo real, nestas arquiteturas de disponibilização de serviços online: "O Facebook precisa realizar um leilão sempre que um usuário acessa seu *feed* de notícias, o que pode gerar mais de um bilhão de leilões em um único dia. Assim, é melhor que esses leilões sejam rápidos!"<sup>33</sup> (ROUGHGARDEN, 2016).

Além da possibilidade de compra, por leilão, de espaços publicitários gerados pelo usuários a partir das suas atividades de utilização dos sistemas digitais pretensamente gratuitos, outras opções são oferecidas aos anunciantes para segmentação do público alvo dos anúncios, o que inclui a localização dos acessos, informações de caracterização pessoal como idade e sexo, além dos seus hábitos de navegação e dos conteúdos compartilhados pelo próprio usuário e pela sua rede de contatos. Ergue-se, portanto, um sistema extremamente sofisticado, capaz de maximizar resultados para anunciantes e plataformas, mantendo o *usuário certo* sempre na mira do *anúncio certo*.

Este complexo sistema produtivo, baseia-se, portanto, essencialmente no tempo dispendido pelos usuários nas aplicações, gerando, a partir do uso, espaços e oportunidades para disponibilização de anúncios que são tão mais eficientes quanto maior for a quantidade de dados pessoais disponíveis para a segmentação do alvo, invariavelmente baseada em perfilização. Para alguns autores, o tempo de alocação, tendo em vista a geração de resultados econômicos para o provedor da plataforma, pode ser encarado como um tempo de trabalho não remunerado, em um mercado monoponista, ou seja, com um único comprador (HASHAI, 2018) e (IBARRA *et al.*, 2018).

A participação ativa do usuário na geração da oportunidade de disponibilização dos espaços publicitários é evidente e uma simples comparação com a televisão torna essa participação ainda mais clara. No caso da TV, independente de existir alguém efetivamente assistindo o canal, a inserção publicitária é apresentada, muito diferente do que acontece com a alocação de espaços nos leilões de anúncios das plataformas digitais, onde o espaço nasce e é negociado em tempo real, a partir da iniciativa do usuário, que é, ao mesmo tempo, gerador da oportunidade, fornecedor dos dados

<sup>32</sup> how do ads on Facebook differ from the basic sponsored search auctions that we've focused on so far? There are many answers to this question. For example, determining which ads are "relevant" in a sponsored search auction is largely determined by the user's search query, whereas Facebook must use other information for this purpose (like a user's friends, recent activity, etc.). Also, ads compete more directly with organic results in Facebook (via its news feed) than in a sponsored search auction. Similarly, real estate devoted to ads is real estate taken away from other things Facebook might want to show you, like friend recommendations. Another difference is that Facebook ads have different sizes and formats, rather than just being sponsored links that each takes up a single slot. Finally, Facebook allows advertisers to bid not only on clicks, but on many other events as well (e.g. likes or downloads of an app). (tradução livre).

<sup>33</sup> Facebook has to run an auction every time a user accesses her news feed, which might be over a billion auctions in a single day. Thus these auctions had better be fast!

peçoais para a escolha dos anúncios que serão apresentados e alvo do anúncio apresentado (produto entregue pela plataforma ao anunciante).

Uma proposta de um novo mercado, lançada por Ibarra *et al.* (2018), sugere uma mudança de perspectiva, de dados como capital, como encaramos os dados atualmente, para dados como trabalho.

Embora possa parecer que os ativos sejam uma coisa ou outra e que o tratamento é irrelevante, as mudanças na atitude social em relação aos ativos nessas categorias têm desempenhado papéis importantes na história. A escravidão e, em menor grau, o feudalismo tratavam o trabalho (em grande parte agrícola) como posse de um senhor ou senhor feudal, enquanto a reforma liberal e trabalhista deu reconhecimento ao trabalho e seu produto econômico marginal.

Dados como Capital (DaC) trata os dados como um resíduo (*exhaust*) da relação de consumo, a ser coletado pela empresa, enquanto Dados como Trabalho (DaL) os trata como algo dos usuários<sup>34</sup> que deve gerar benefícios primeiramente para eles<sup>35</sup>.

Os autores também destacam que apenas poucas pessoas têm consciência da geração de valor a partir dos seus próprios dados, pelos serviços digitais oferecidos gratuitamente, o que cria um caso extremo de monopólio, onde ao invés de diminuir o preço, as empresas, reforçando a ideia de DaC e apoiando-se na falta de conhecimento dos usuários sobre o valor dos seus dados, simplesmente não pagam nada.

Obviamente, há uma tendência de manutenção da perspectiva DaC, tendo em vista que grandes estruturas econômicas se beneficiam deste modelo, mas os autores indicam alguns pontos de pressão que podem tornar efetiva a mudança de perspectiva. Primeiro, a ação de outros grandes competidores, que não estão predominantemente focados em serviços digitais gratuitos para os usuários, como Amazon, Apple e Microsoft, que podem incentivar novos paradigmas para aumentarem suas capacidades de atuação na corrida pela consolidação de tecnologias ligadas a Inteligência Artificial. Aqui vale uma nota: dois dos cinco autores do paper, Jaron Lanier e Glen Weyl, possuem vínculo direto com a Microsoft. Em segundo lugar, apontam a necessidade de criação de um sindicato de usuários ("*data labor union*") que possa barganhar de modo mais equilibrado com as grandes empresas *consumidoras* de dados pessoais. Finalmente, apontam a ação dos governos no sentido de facilitar do DaL, seja criando legislações que garantam direitos aos usuários e exijam que os grandes *players* ofe-

<sup>34</sup> No original as user possession. Optou-se por esta tradução por considerar inadequada a tradução mais direta, relacionada a posse ou propriedade, termos com grande carga jurídica não explícita no texto original

<sup>35</sup> Texto original: "While it might seem that assets either are one or the other, and that treatment is irrelevant, transitions in the social attitude towards assets across these categories have played important roles in history. Slavery and to a lesser extent feudalism treated (largely agricultural) work as a possession of a master or lord, while liberal and labor reform worked to give recognition and its marginal economic product to labor. DaC treats data as natural exhaust from consumption to be collected by firms, while DaL treats them as user possessions that should primarily benefit their owners."(tradução livre)

reçam informações sobre como, por que e em que circunstâncias os dados pessoais são utilizados, caso do GDPR europeu; seja pela reforma das legislações trabalhistas, de forma a alinhá-las à nova realidade trazida pela economia de dados; seja, por fim, pela ação direta contra mercados monopsônios (IBARRA *et al.*, 2018).

Mesmo que uma mudança radical não se concretize, fica evidente uma extrema apropriação, pelos grandes provedores de serviços digitais pretensamente gratuitos, não apenas dos dados pessoais dos usuários, sejam estes intrínsecos ou gerados como resultado da própria atividade online, mas também do tempo alocado pelos usuários na utilização das plataformas que, em última análise, cria as oportunidades de alocação dos anúncios, leiloados para as empresas anunciantes.

Apesar de grandes avanços alcançados nos últimos anos, legislações de proteção de dados abordam especificamente a forma como os dados pessoais são utilizados. O foco evidente está no tratamento e não diretamente nos resultados econômicos obtidos por este tratamento, apesar da finalidade ser um aspecto relevante para o enquadramento de uma determinada atividade de tratamento como lícita. Neste sentido, pode ser necessária a existência de novas abordagens regulatórias, capazes de atingir não apenas as atividades de tratamento em si, mas também o resultado final obtido, pensando o usuário, na atividade de uso, como um fator relevante de produção ou criando a possibilidade, para o usuário, de não participar da cadeia de produção.

### 2.2.2 Da economia do encontro à economia da vigilância

Uma definição enciclopédica, quase verbete de dicionário, de Capitalismo da Vigilância, abre a obra de Shoshana Zuboff (2019), sobre o tema:

#### **Sur-veil-lance Cap-i-tal-ism, n.**

1. Uma nova ordem econômica que assume a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e vendas; 2. Uma lógica econômica parasitária na qual a produção de bens e serviços está subordinada a uma nova arquitetura global de modificação de comportamento; 3. Uma mutação desonesta do capitalismo marcada por concentrações de riqueza, conhecimento e poder sem precedentes na história humana; 4. A estrutura fundamental de uma economia de vigilância; 5. Uma ameaça tão significativa à natureza humana no século XXI quanto o capitalismo industrial foi para o mundo natural nos séculos XIX e XX; 6. A origem de um novo poder instrumentalista que reivindica domínio sobre a sociedade e apresenta desafios surpreendentes à democracia de mercado; 7. Um movimento que visa impor uma nova ordem coletiva com base na certeza total; 8. Uma expropriação de direitos humanos cruciais, que é melhor entendida como um golpe: uma derrubada da soberania do povo<sup>36</sup>.

<sup>36</sup> Texto original: "1. A new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales; 2. A parasitic economic logic in which the production of goods and services is subordinated to a new global architecture of behavioral modification; 3. A rogue mutation of capitalism marked by concentrations of wealth, knowledge, and power unprecedented in human history; 4. The foundational framework of a surveillance economy; 5. As significant a threat to human nature in the twenty-first century as industrial capitalism was

Ao delinear a lógica e a forma de operacionalização do Capitalismo de Vigilância, Zuboff utiliza o Google como paradigma. Geralmente considerado como uma plataforma bilateral (*two-sided platform*) ou multilateral (*multi-sided platform*), a autora discorda deste enquadramento. Argumenta que serviços como o Google transformam suas interações “fora de comércio” (*nonmarket*), realizadas com os usuários, em matéria prima para a fabricação de produtos que visam transações de mercado genuínas, com seus reais clientes, os anunciantes, ou seja, essa transação de um excedente comportamental (*behavioral surplus*) de fora para dentro de um mercado possibilita ao Google converter investimento em receita. Inicialmente ligados às buscas, novos produtos de predição foram disponibilizados e passaram a ser vendidos pela empresa, em larga escala baseada na matéria prima obtida por meio de mecanismos de vigilância, que podem ser denominados como ativos de vigilância (*surveillance assets*). E conclui:

Esses ativos são matérias-primas essenciais na busca por receitas de vigilância e sua conversão em capital de vigilância. Toda a lógica dessa acumulação de capital é entendida com mais precisão como capitalismo de vigilância, que é a estrutura fundamental para uma ordem econômica baseada em vigilância: uma economia de vigilância<sup>37</sup>.

Apesar de didático, o modelo proposto por Zuboff, em que duas engrenagens, uma funcionando sob uma ótica de mercado, oportunisticamente com base na captação de dados gerados por relações fora de mercado (*nonmarket*), criando um excedente comportamental, aparenta ser extremamente simplificador. Ao olhar a oferta destas empresas com "produtos de predição que aumentam as taxas de clique para publicidade orientada (*targeted advertising*)", despreza, em grande medida, o fato de que grande parte das interações das plataformas, tanto com os usuários quanto com os anunciantes acontecem, em tempo real, no tempo de utilização da plataforma. Também não leva em consideração os complexos ecossistemas de aplicações construídos sobre diversas plataformas. Os sistemas digitais que baseiam seu funcionamento em dados pessoais não é monolítico, nem ao se considerar uma única plataforma. Muitas vezes, é formada por emaranhados de serviços, executados por terceiros, a maioria deles submersos, para se chegar a um resultado visível ao usuário. Pensar dois processos paralelos despreza boa parte da imensa complexidade destes modelos de negócio.

---

to the natural world in the nineteenth and twentieth; 6. The origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy; 7. A movement that aims to impose a new collective order based on total certainty; 8. An expropriation of critical human rights that is best understood as a coup from above: an overthrow of the people's sovereignty."(tradução livre)

<sup>37</sup> Texto original: "These assets are critical raw materials in the pursuit of surveillance revenues and their translation into surveillance capital. The entire logic of this capital accumulation is most accurately understood as surveillance capitalism, which is the foundational framework for a surveillance-based economic order: a surveillance economy"(tradução livre)

Zuboff também defende a ideia de que os grandes players que baseiam seus modelos de negócio na vigilância buscam por espaços sem regulação. Nas suas palavras:

É importante entender que os capitalistas da vigilância são impelidos a buscar espaços sem regulação (lawlessness) pela lógica de sua própria criação. (...) O código é a lei para o Google agora, mas o risco de novas leis em seus territórios estabelecidos e projetados continua sendo um perigo persistente para o capitalismo de vigilância. Se novas leis proibissem as operações de extração, o modelo de vigilância implodiria<sup>38</sup>. (ZUBOFF, 2019)

Sobre este ponto Julie E. Cohen faz uma crítica precisa, ressaltando que a relação destas empresas com a produção normativa é bem mais complexa e produtiva do que a delineada Zuboff. Para ela, os atores da economia da informação não agem apenas no mercado, mas também mobilizam as ferramentas legais e institucionais para avançarem em seus objetivos. Assim, "instituições legais não são simples superestruturas, mas sim meios através dos quais expressões de racionalidade econômica tornam-se específicas, detalhadas e acionáveis"(COHEN, 2019c).

Cohen (2018) identifica que as práticas de processamento de informações pessoais constituem um novo tipo de domínio público, que chamou de domínio público biopolítico. Um repositório de matérias-primas que são extraídas e formatadas como insumos (*inputs*) para um tipo específico de atividade produtiva. Ressalta, também, que essa matéria-prima não é meramente pessoal ou informacional, mas sim biopolítica, porque as atividades produtivas que a utilizam envolvem a descrição, processamento e gerenciamento de populações, com consequências que são produtivas, distributivas e epistemológicas, agindo de duas formas complementares e interrelacionadas:

Primeiro, constitui informação pessoal como disponível e potencialmente valiosa: como um conjunto de materiais que podem ser apropriados livremente como insumos para a produção econômica. Esse enquadramento apoia a reorganização da atividade sociotécnica de maneira direcionada à extração e apropriação. Segundo, o domínio público biopolítico constitui como brutas [não processadas] as informações pessoais coletadas em ambientes de informações em rede.<sup>39</sup>

A construção proposta por Cohen é especialmente feliz ao expor a existência de uma fronteira, geralmente obscura, entre os dados pessoais, como o insumo original, bruto e disponível para apropriação, e o resultado do tratamento destes dados, este

<sup>38</sup> No original: "It is important to understand that surveillance capitalists are impelled to pursue lawlessness by the logic of their own creation. (...) Code is law for Google now, but the risk of new laws in its established and anticipated territories remains a persistent danger to surveillance capitalism. If new laws were to outlaw extraction operations, the surveillance model would implode."(tradução livre)

<sup>39</sup> Texto original: "First, it constitutes personal information as available and potentially valuable as a pool of materials that may be freely appropriated as inputs to economic production. That framing supports the reorganization of sociotechnical activity in ways directed toward extraction and appropriation. Second, the biopolitical public domain constitutes the personal information harvested within networked information environments as raw"(tradução livre).

de caráter privado, fruto de uma atividade produtiva complexa e que, por este motivo, é passível de uma proteção que se estende além dos mecanismos de tratamento em si, em geral protegidos por propriedade intelectual, atingindo inclusive este resultado da apropriação, sendo muitas vezes consideradas, a informação propriamente ou a sequência de atividades de processamento utilizadas para alcançá-lo, segredo industrial ou comercial.

Os termos de uso, em geral, são os instrumentos jurídicos utilizados para garantir a legalidade dessa transferência dos dados, do domínio público para o domínio privado, em um processo essencialmente performático, pois o aceite dos termos funciona como uma rotina de interação comercial, com uma forma contratual, mas operacionalmente mandatório, já que são implementados como contratos de adesão (*boilerplate agreements*) (COHEN, 2019a).

Também apresenta uma visão mais abrangente e precisa do modo como os players da economia da informação agem e interferem no processo de construção das bases de legalidade de suas atividades, criando uma “lógica jurídica” adequada e convincente. Este esforço articulado, denominado por Cohen de empreendedorismo legal-institucional (*legal-institutional entrepreneurship*), alinha-se como a própria forma de organização do Estado, em regimes neo-liberais, onde os métodos administrativos regulatório tradicionais são substituídos por mecanismos regulatórios de caráter gerencial (COHEN, 2019c).

Outro aspecto relevante do “empreendedorismo legal-institucional” refere-se à participação de entidades não estatais (com ou sem fins lucrativos) e orientadas por múltiplos stakeholders, como a IETF (Internet Engineering Task Force), a ICANN (Internet Corporation for Assigned Names and Numbers), a International Telecommunications Union e a IEEE (Institute of Electrical and Electronic Engineers), que determinam protocolos e processos a serem seguidos pela indústria e, em grande medida, definem o modo de funcionamento e estrutura da rede. Este tipo de estruturação permite que as empresas tenham participação direta no processo decisório, podendo influir diretamente na regulação técnica (COHEN, 2019b).

Assim, as novas modalidades regulatórias, que estão sendo estruturadas para suportar a economia da informação, são “processualmente informais, mediadas por redes de conhecimento técnico e profissional que definem padrões relevantes, fortemente dependentes de estratégias de privatização e automação e opacas à observação externa”<sup>40</sup> (COHEN, 2019c).

A descrição sugerida por Cohen pode ser observada, também, no âmbito das estruturas de proteção de dados, principalmente ao observar-se o paradigma europeu, com entidades como o Comitê Europeu para a Proteção de Dados (EDPB) e a Asso-

<sup>40</sup> Texto original: “procedurally informal, mediated by networks of professional and technical expertise that define relevant standards, heavily reliant on privatization and automation strategies, and opaque to external observation.”(tradução livre)

ciação Internacional dos Profissionais de Privacidade (IAPP). Sem poder normativo coercitivo direto, atuam como pontos importantes de influência e de definição de padrões, que são irradiados para todo o espectro do sistema de regulação, incluindo as autoridades nacionais de proteção de dados.

Uma mudança significativa também acontece entre os órgãos reguladores e os agentes de mercado. A função clássica de supervisão, com poder coercitivo, dos órgãos governamentais responsáveis pela fiscalização das atividades realizadas por estes agentes, agora alinha-se a uma postura colaborativa, necessária em sistemas onde parte das atividades de conformidade é "terceirizada" para a própria organização fiscalizada. Um exemplo característico desta postura colaborativa são os guias, recomendações e melhores práticas emitidas por agências e autoridades reguladoras. Como resume Cohen: "Processos colaborativos (ou co-regulatórios) tipicamente culminam em padrões consensuais de melhores práticas, que visam orientar o *compliance* e o *enforcement*, e podem confiar significativamente em auto-regulamentação e *enforcement* privado"<sup>41</sup> (COHEN, 2016).

Também neste ponto é possível observar grande similaridade entre o cenário descrito por Cohen e o arranjo de *enforcement* regulatório observado, na Europa, para proteção de dados pessoais. Algumas autoridades nacionais, como a Commission Nationale de l'Informatique et des Libertés (CNIL), da França, e a Information Commissioner's Office (ICO), do Reino Unido, juntamente com organismos como o EDPB atuam como grandes emissores de padrões, influenciando não apenas a forma de estruturação dos programas de conformidade das empresas, mas também outras autoridades nacionais e órgãos de controle, além de promoverem influências mútuas.

A transferência das responsabilidades de controle para a própria organização controlada também é explícita nos textos normativos. Não é raro, na literatura especializada em privacidade e proteção de dados, os próprios textos legais serem citados como *frameworks*, bases para a criação e manutenção de estruturas internas de conformidade. Assim, as linhas gerais dos mecanismos internos de controle são estabelecidas pela legislação de base e o seu recheio é preenchido pelos guias e orientações emitidos pelas autoridades ou órgãos auxiliares, muitos deles multi-setoriais ou organizações profissionais.

Esta estruturação cria um ambiente de maior tranquilidade para os *players* de mercado. Em grande medida, este modelo de regulação também age como facilitador de processos internos, muitas vezes difíceis de serem implementados. Um exemplo bastante didático deste efeito é descrito no livro *Tools and Weapons*, escrito por Brad Smith, presidente e CLO (Chief Law Officer) da Microsoft, e Carol Ann Browne, Diretora Sênior de Relações Externas e Comunicação, também da Microsoft.

<sup>41</sup> Texto original: "Collaborative (or coregulatory) proceedings typically culminate in consensus best-practice standards intended to guide both compliance and enforcement, and may rely significantly on self-regulation or private enforcement" (tradução livre)



No capítulo sobre privacidade dos consumidores, há uma descrição da reunião de apresentação do plano de adequação da Microsoft à GDPR, um projeto que envolveria mais de trezentos engenheiros, em tempo integral, com duração de, no mínimo, dezoito meses, com um esforço intensivo nos seis últimos meses, que poderia chegar a envolver mais de mil, com um comprometimento financeiro na casa das centenas de milhões de dólares. A certa altura da reunião, Satya Nadella, CEO da Microsoft, disse: “Isso não é ótimo? Durante anos, foi quase impossível conseguir que todos os engenheiros da empresa concordassem com uma única arquitetura de privacidade. Agora os reguladores e advogados nos disseram o que fazer. O trabalho de criar uma única arquitetura ficou muito mais fácil”<sup>42</sup> (SMITH; BROWNE, 2019).

Expandir a percepção do capitalismo de vigilância para o capitalismo informacional, em que a vigilância deve ser encarada como um aspecto fundamental da teoria de economia política que sustenta este novo padrão, onde os atores de mercado atuam, não apenas no desenvolvimento de suas plataformas, que se capilarizam lógica e fisicamente, mas também agem, ativamente, na conformação das estruturas de regulação a que suas atividades estarão sujeitas, não significa uma diminuição da importância ou da relevância da vigilância. Caracteriza-se como um importante marco conceitual que explicita relações muitas vezes encobertas por aforismos e frases de impacto, mais próximas do ativismo do que do esclarecimento, como ocorre na definição fixada por Zuboff, logo no começo do seu livro.

### 2.2.3 Quem paga pelo tempo livre?

Em 1.996, George Gilder fez uma previsão impressionante, em um artigo publicado na revista *Wired*:

Transcendendo todos os conceitos anteriores de centralização e descentralização, uma máquina global distribuirá o processamento no ponto ideal e acessará tudo. Alimentando-se de baixa potência e alta largura de banda, o computador mais comum da nova era será um telefone celular digital com um endereço IP <sup>43</sup> (GILDER, 1996).

Articulando, de modo absolutamente especulativo, os conceitos de escassez e abundância, no que ele auto-intitulou *Paradigma de Gilder*, seu exercício de futurologia não só acertou, em uma época onde não se atribuía IPs a telefones celulares, que estes seriam os principais equipamentos de conexão e processamento local de informação com interação homem-máquina, mas também conseguiu visualizar a articulação de

<sup>42</sup> Texto original: “Isn’t this great? For years it has been next to impossible to get all the engineers across the company to agree on a single privacy architecture. Now the regulators and lawyers have told us what to do. The job of creating a single architecture just got a whole lot easier.” (tradução livre)

<sup>43</sup> Texto original: “Transcending all previous concepts of centralization and decentralization, one global machine will distribute processing to the optimal point and access everything. Feeding on low power and high bandwidth, the most common computer of the new era will be a digital cellular phone with an IP address.” (tradução livre)

um grande poder computacional central capaz de receber os dados e prover serviços para estes terminais, a que deu o nome de "máquina global".

Mesmo que frustrada a tentativa de resumir toda uma teoria econômica em uma frase, o grande acerto de Gilder foi apostar na capacidade de cientistas da computação, engenheiros, físicos e químicos em transformar escassez em abundância ou de, na impossibilidade desta transformação, articular os bens escassos de uma forma bastante eficiente. Dois exemplos explicitam esta capacidade.

O primeiro diz respeito à própria Lei de Moore: "o número de transistores em um chip aproximadamente dobrará a cada 24 meses". Criada por Gordon Moore, um dos fundadores da Intel, esta previsão continua sendo confirmada há mais de 50 anos. Pode ser difícil, a primeira vista, entender a escala exponencial deste enunciado, mas os números comparativos ajudam a esclarecer. O primeiro processador Intel, o Intel 4004, lançado em 1.971, possuía 2.300 transistores (INTEL CORPORATION, s.d.). Atualmente, o processador embarcado no iPhone 11 Pro, da Apple, possui 8.500.000.000 de transistores (APPLE, 2019). O tamanho dos transistores também ajuda a entender a curva de evolução imposta pela Lei de Moore: enquanto o primeiro transistor, produzido no Bell Labs, em 1947, podiar ser pego com a mão, o transistor do processador A13 Bionic, chip embarcado no mesmo iPhone 11 Pro, mede 7 nanômetros. Vale lembrar que 1 milímetro é dividido em 1.000.000 de nanômetros. Em 2.019, a Cerebras anunciou o lançamento do primeiro chip com mais de 1 trilhão de transistores (1,2 trilhão), desenvolvido para processamento de sistemas de inteligência artificial (SARACCO, 2019).

O segundo exemplo está ligado a energia. Em 2019, o Prêmio Nobel de Química foi dividido por três cientistas: John B. Goodenough, M. Stanley Whittingham e Akira Yoshino. Com pesquisas iniciadas nas décadas de 1970 e 1980, eles contribuíram de modo fundamental para o desenvolvimento das baterias de íon-lítio, cuja comercialização teve início em 1.991 e que hoje dominam as aplicações, de celulares a carros. A importância desta tecnologia vai além de possibilitar a explosão de mobilidade que experimentamos atualmente, garantindo energia para telefones celulares, câmeras e até veículos, desde patinetes até aviões, passando por ônibus e caminhões. A eficiência de armazenamento de energia, em grande medida consequência destas pesquisas, também figura como um importante elemento de complementação a fontes flutuantes de energia, como o vento e a luz solar. Com as baterias, a demanda por energia pode ser atendida mesmo em situações onde nenhuma energia pode ser produzida (THE ROYAL SWEDISH ACADEMY OF SCIENCES, 2019).

Mas há um fator de escassez muito mais difícil de manejar e que está no centro da evolução dos serviços digitais disponibilizados gratuitamente: o tempo! O tempo dos usuários afeta, diretamente, duas das três posições concomitantes ocupadas por alguém que utiliza estes serviços. Quanto mais tempo conectado, maior a quantidade

de dados pessoais captados (melhor eficiência da fonte geradora de matéria-prima) e também maior a exposição às mensagens e mecanismos de marketing, ou seja, maior a eficiência do serviço na entrega de publicidade (usuário como produto). Neste sentido, o aumento da eficiência destes mecanismos de geração de valor baseado no uso de aplicação sem pagamento direto pelos usuários está, em grande medida, associado ao aumento do tempo de exposição, direta ou indireta (importante sempre lembrar das estratégias de capilaridade lógica, como *embed codes*, já abordados anteriormente), dos usuários ao conjunto de aplicações disponibilizada por um determinado *player*.

A economia da vigilância é uma das formas de aumentar o tempo de permanência dos usuários em contato com estes serviços, mas pode ainda não ser suficiente. Pode ser necessário, em uma próxima fronteira, enfrentar a questão da geração de renda.

Albert Wenger<sup>44</sup>, sócio da Union Square Ventures, uma das grandes gestoras de capital de risco do mundo, com investimentos realizados em empresas como Twitter, Duolingo, Soundcloud, Kickstarter, Foursquare e Zynga, em evento realizado no ano de 2015, ao tratar dos impactos da ideia de custo marginal zero, fenômeno muito característico dos serviços digitais, indicou a necessidade, sob o seu ponto de vista, de uma inversão nas políticas públicas (WENGER, 2015). A primeira dessas mudanças seria a criação do que ele designou de “BIG” (*Basic Income Guarantee*, ou garantia de renda básica), uma renda universal distribuída indistintamente para toda a população, de forma a garantir suas necessidades básicas. Em seguida, Wenger apresenta qual a inversão sugerida: atualmente as pessoas trabalham primeiro para depois terem seu pagamento, já no novo modelo elas receberiam primeiro e depois decidiriam em que (ou se) trabalhariam. Assim, a renda advinda do trabalho se tornaria uma renda complementar, permitindo que as pessoas passassem a dispor de mais tempo, tudo isso sendo possível porque grande parte das atividades humanas será substituída pelas máquinas. E completa:

Então, em um mundo de abundância digital, nós queremos que as pessoas tenham tempo, nós queremos que as pessoas sintam que elas têm o tempo e os recursos necessários para aprender novas coisas, que elas tenham o tempo e os recursos necessários para contribuir com estas coisas e que, então, sejam livres. (WENGER, 2015)

Já em 2019, na Conferência Anual do Trabalho, organizada pela Escola de Direito da Universidade de Nova Iorque (NYU School of Law), dedicada aos impactos da Inteligência Artificial e da Automação no Trabalho e na Vida dos Trabalhadores, em um *workshop* chamado “Programas de Mitigação de Impactos para os Trabalhadores” (*Programs in mitigation of impact on workers*), Wenger reforçou a ideia da Renda Básica Universal (UBI) como uma medida necessária, mas não suficiente, para ingresso

<sup>44</sup> Albert Wenger é autor do livro digital *World After Capital*, que consta nas referências bibliográficas.

no que ele intitula de “Era do Conhecimento”, superando definitivamente a “Era Industrial”. Além disso, traz uma abordagem sobre a renda universal como uma forma de financiar um novo modelo de alocação da atenção humana, atualmente concentrada, essencialmente, no trabalho e sugere um novo enquadramento do tema, deslocando a vista da mitigação dos impactos da automação para se enxergar o conceito sob a ótica da liberdade, da liberdade econômica ou, em outras palavras, liberdade para alocação do próprio tempo, seja na busca por um incremento da renda, com o trabalho, seja realizando outras atividades, essencialmente humanas, não geradoras de renda (WENGER, 2019).

O que Wenger não diz é que, enquanto as pessoas aprendem e se divertem no meio digital, em um mundo de abundância digital, seus dados pessoais estão sendo capturados, armazenados e processados para tornar estes serviços mais eficientes para seus verdadeiros objetivos, transformando as pessoas, que aprendem e se divertem, em alvos mais alinhados às campanhas publicitárias que efetivamente financiam estes serviços em extrema abundância.

E esta não é uma ideia isolada. Grandes nomes da indústria dos serviços digitais e das novas tecnologias, como Mark Zuckerberg, Elon Musk (SÔNECO; CALDAS, 2017), Marc Andreessen e Tim O’Reilly (SADOWSKI, 2016) alinham-se a Wenger e defendem a mesma ideia. A Y Combinator, considerada a melhor aceleradora de startups do mundo em 2017, pelo ranking da revista Forbes (KONRAD, 2017), anunciou a realização de um experimento na cidade de Oakland, na Califórnia, envolvendo 100 famílias que receberam entre US\$ 1.000 e US\$ 2.000 mensais, por seis meses, para a validação do conceito de renda básica universal. Não é de se estranhar que uma aceleradora de startups utilize, para políticas públicas, o mesmo modelo de teste de validação dos produtos que acelera (SADOWSKI, 2016).

Encerrado o piloto, realizado em Oakland, a Y Combinator inicia uma nova fase do projeto, agora em parceria com a Universidade de Michigan. Assim como Wenger, a iniciativa de pesquisa da aceleradora também vê na renda básica como peça chave de um novo contrato social para o século XXI. Em um site dedicado ao projeto, a aceleradora apresenta o seu plano:

Estamos trabalhando com os principais especialistas em economia, saúde pública e outros campos e estabelecendo parcerias com agências governamentais para coletar dados administrativos precisos. Medir como as pessoas gastam seu tempo e dinheiro, indicadores de saúde mental e física e efeitos em crianças e redes sociais nos ajudará a aprender como esse nível básico de segurança econômica ajuda as pessoas a lidar - e até prosperar - em meio a volatilidade e incerteza<sup>45</sup> (YC RESEARCH, s.d.).

<sup>45</sup> Texto original: "We're working with leading experts in economics, public health, and other fields and partnering with government agencies to collect precise administrative data. Measuring how individuals spend their time and money, indicators of mental and physical health, and effects on children and social networks will help us learn how this basic level of economic security helps people cope—and even thrive—in the midst of volatility and uncertainty."(tradução livre).

A forma da alocação do tempo, como se pode observar, é um dos fatores de análise da pesquisa. No documento de detalhamento do projeto, na seção Perguntas de Pesquisa (*Research Questions*), a pergunta número um é: "Como a renda básica recebida afeta a maneira como as pessoas dispõem seu tempo?"<sup>46</sup>, e o texto continua com o seguinte detalhamento:

A teoria econômica convencional prevê que indivíduos que estão recebendo uma renda básica dispenderão menos tempo trabalhando. O que eles estão fazendo com esse tempo? Utilizaremos pesquisas on-line frequentes para obter imagens detalhadas do uso do tempo - por exemplo, as horas trabalhadas diminuem e, em caso afirmativo, as pessoas usam o tempo extra para dormir e se dedicar a mais atividades de lazer, ou passam mais tempo com as crianças ou buscam educação e treinamento adicionais? Eles continuam trabalhando, mas optam por empregos com salários mais baixos, mas mais gratificantes ou que mais os satisfaçam? Investimentos em capital humano e físico, como resultados de educação, trabalho autônomo e empreendedorismo, também fazem parte desse conjunto de perguntas<sup>47</sup> (Y COMBINATOR RESEARCH, 2017).

No mesmo documento, a YC Research, iniciativa sem fins lucrativos da Y Combinator, detalha os resultados esperados para todas as perguntas de pesquisa estabelecidas. Ao tratar especificamente da alocação do tempo, o estudo pretende identificar mudanças em quatro categorias de atividades: (i) atividades remuneradas, incluindo mudanças nos padrões de trabalho, como busca por ocupações que geram maior satisfação (troca de trabalhos de baixa qualidade por trabalhos de alta qualidade), trabalho autônomo, trabalhos secundários e empreendedorismo; (ii) investimento em capital humano, com atividades de educação e treinamento para a própria pessoa ou para membros da família; (iii) atividades produtivas não remuneradas, como cuidados com crianças ou idosos, voluntariado ou engajamento com atividades cívicas e comunitárias; (iv) atividades de lazer (Y COMBINATOR RESEARCH, 2017). Compreender a alocação do tempo, em uma realidade onde exista garantia de renda suficiente e constante para sustentar um padrão de vida digno, sem a necessidade de dispender tempo de trabalho, é fundamental para projetar a evolução dos serviços digitais, considerando a redução extrema da alocação homem-hora que se avizinha, em especial nos países desenvolvidos.

Mais do que a busca por um novo contrato social, pela concretização de uma liberdade material e não apenas formal, ou pela minimização dos impactos da automação intensiva decorrente do avanço tecnológico, em especial da inteligência artificial,

<sup>46</sup> Texto original: "How does receiving a basic income affect the way people spend their time?"(tradução livre)

<sup>47</sup> Standard economic theory predicts that individuals who are receiving a basic income will spend less time working. What are they doing with that time instead? We will leverage frequent online surveys to obtain detailed pictures of time use — e.g. do hours worked decrease and, if so, do people use the extra time to sleep and engage in more leisure, or do they spend more time with children or pursue further education or training? Do they continue to work but choose lower-paid but more fulfilling or more satisfying jobs? Investments in human and physical capital such as educational outcomes, self-employment, and entrepreneurial activities are also integral to this set of questions.

que tende a substituir ocupações até então exclusivamente humanas, o discurso e os esforços das grandes organizações do ecossistema de tecnologia da informação escondem objetivos econômicos mais diretos.

Sob o manto de uma ideia de liberdade, de diminuição da pobreza e das incertezas decorrentes da disponibilidade mais fluida de trabalho esconde-se, na realidade, o desejo de financiamento de toda uma indústria a partir da socialização dos custos a ela associados. Uma mudança que socializa o risco dos empreendimentos digitais e, concomitantemente, concretiza a ideia de transformar os seres humanos, verdadeiramente, em grandes usinas de dados, maximizando seu tempo de disponibilidade da mesma forma com que se maximiza o tempo de produtividade de uma refinaria de petróleo.

### 2.3 *NÓS NÃO VAMOS PAGAR NADA, É TUDO FREE*

Existe uma máxima muito comum de ser escutada no ecossistema de inovação e empreendedorismo: peça desculpas, não peça licença. Na prática, isso acontece em um amplo espectro de situações, que vão de excessos não previsíveis a violações intencionais de regras, que ora se alinham a um comportamento de desobediência civil, ora flertam ou ultrapassam os limites da ética e da legalidade, como no caso clássico do uso da infraestrutura de Harvard, por Bill Gates e Paul Allen, este último que nem possuía vínculo com a universidade, em especial um PDP-10 financiado pelo departamento de defesa americano, para o desenvolvimento da primeira versão do Basic. Isso rendeu um processo disciplinar contra Gates, pelo uso indevido da máquina e por permitir a entrada de Allen, no laboratório, com a sua senha. Foi absolvido pelo uso do PDP-10, mas advertido pela liberação de acesso ao laboratório por alguém de fora da universidade. Além disso, teve que aceitar disponibilizar a primeira versão do Basic em domínio público (ISAACSON, 2014).

Em grande medida, a ideia contida nesta máxima é inerente à inovação. Empurrados pela Lei de Moore, a inovação disruptiva cria circunstâncias difíceis de serem imaginadas a priori e, por este motivo, impossíveis de serem reguladas. Eric Schimdt, então CEO do Google, em uma entrevista dada ao *The Wall Street Journal*, em 2011, relembra uma frase que ouviu de Andy Grove, um dos fundadores da Intel, em um jantar, em 1995, que explica bem esse descompasso, “É fácil de entender. Negócios de alta tecnologia são três vezes mais rápidos do que negócios convencionais. E os governos são três vezes mais lentos que os negócios convencionais. Então nós temos uma diferença de nove vezes”<sup>48</sup> (CROVITZ, 2011).

Já do ponto de vista econômico, mesmo baseado simplesmente no senso co-

<sup>48</sup> Texto original: “This is easy to understand. High tech runs three times faster than normal businesses. And the government runs three times slower than normal businesses. So we have a nine-times gap” (tradução livre)

num, é relativamente fácil concluir que reproduzir informação é muito mais barato do que criá-la. No jargão econômico, produtos informacionais possuem alto custo fixo e baixo custo marginal. Esta estrutura de custo, como explicam Shapiro e Varian (1999), possui implicações importantes, dentre elas está a forma de determinação do preço, que não está ligado ao custo de produção (ou reprodução), mas sim ao valor que o consumidor está disposto a pagar por ela.

E qual é esse preço? Esta é uma pergunta central e que, para os sistemas digitais oferecidos gratuitamente, é respondida por complexos sistemas de leilão capazes de alocar, em tempo real, espaços de publicidade para um público altamente segmentado. Mas existe uma outra pergunta, que possui uma resposta atterradoramente óbvia, mas que também é fundamental: quanto vale uma informação que ninguém conhece?

Enquanto, no Lado B das plataformas, existe um sistema complicado e lucrativo de monetização de dados pessoais, no Lado A, os usuários consomem conteúdos que, massivamente, não foram produzidos diretamente pelas plataformas, mas que foram gratuitamente disponibilizados por outros usuários ou capturados diretamente da internet, rearranjados, e disponibilizados de uma outra forma, também sem nenhum tipo de remuneração. E por que isso acontece? Porque há um ganho efetivo, muitas vezes não monetário, para aqueles que disponibilizam diretamente ou permitem a redistribuição de suas informações por estas plataformas. Seja pelo aumento da relevância de um conteúdo profissionalmente criado, seja para criação de novas oportunidades de venda, seja para valorização pessoal no mercado da imagem e da boa vida nas redes sociais, sempre existe um cálculo econômico, mesmo que inconsciente, na disponibilização direta e voluntária das informações explicitamente expostas pelas plataformas.

Já se o cálculo está correto, se os ganhos superam os custos, se os riscos valem a pena, são questões cujas respostas ficam reservadas a cada produtor de conteúdo, o que não impede a existência de reações ou de ações coordenadas, na busca por um novo equilíbrio entre produtores de informação e plataformas. Não é apenas no lado escondido da manipulação dos dados pessoais que as lutas estão sendo travadas. Elas acontecem, também, à luz do sol, na oferta dos serviços primários que são disponibilizados gratuitamente para os consumidores.

### **2.3.1 Apropriação de conteúdo**

No final da década de 1990, era pouco crível, para usar uma expressão eufemista, a ideia de capturar toda a web, ou uma grande parte dela, para se criar um sistema de busca eficiente. Dennis Allison, professor Stanford, resumiu de maneira precisa a empreitada:

A idéia de digitalizar todo o universo e fazê-lo funcionar é algo que ninguém estava disposto a enfrentar, mas muita gente sabia que precisava ser feito.

Eles conseguiram reunir isso e destruíram as limitações. E com um pouco de sorte, isso realmente vai funcionar<sup>49</sup> (VISE; MALSEED, 2018).

Desde o princípio, quando ainda era um projeto que rodava na infraestrutura de Stanford, a ideia central do Google sempre foi armazenar e processar todo o conteúdo das páginas atingidas pelo buscador. Em uma apresentação de Page e Brin, na universidade, organizada por Allison, em setembro de 1998, Page disse: “Nós, atualmente, armazenamos todas as páginas que baixamos porque isso é muito bom para pesquisa. Nós temos a Web em discos do outro lado do hall” (VISE; MALSEED, 2018). Já existia, também, naquela época, uma consciência por parte de Page e Brin sobre o potencial de manipulação dos resultados, explicitado em um paper escrito pela dupla, juntamente com Motwani e Winograd, em 1999, apesar de considerarem os PageRanks personalizados, como base de classificação, imunes de manipulação direta e apenas suscetível a manipulações indiretas (PAGE *et al.*, 1999), por compra de links em páginas indexadas. Ainda era cedo para prever a indústria do Search Engine Optimization (SEO) que foi construída a partir da ascensão dos buscadores.

Uma característica relevante da web, que favoreceu a apropriação de conteúdos de terceiros e seu tratamento computacional, é o fato de que o Hypertext Markup Language (HTML)<sup>50</sup> é, por construção, *open source* (VARIAN; FARRELL; SHAPIRO, 2004). Isso significa que qualquer usuário pode, diretamente no *browser*, ver o código que forma a página. Assim, é possível varrer a web, de página em página, identificando de modo relativamente simples, todas as suas partes, o que inclui os links, os títulos, as âncoras etc. O *paper* de 1998, escrito por Page e Brin, que apresenta formalmente o sistema de busca explica de forma didática como isso acontece:

No Google, o rastreamento da web (*download* das páginas web) é feito por muitos rastreadores distribuídos. Há um servidor de URLs (*URLserver*) que envia listas de URLs a serem buscadas pelos rastreadores. As páginas web obtidas são, então, enviadas para o *storeserver* (servidor de armazenamento). O *storeserver* então comprime e armazena as páginas web em um repositório. Toda página web é associada a um número de identificação (ID) chamado docID que é associado a toda nova URL que é analisada de uma página web. A função de indexação é executada pelo indexador (*indexer*) e pelo classificador (*sorter*). O indexador executa um conjunto de funções. Ele lê o repositório, descomprime os documentos e os analisa. Cada documento é convertido em um conjunto de ocorrências de palavra chamados de *hits*. Os *hits* registram a palavra, posição no documento, uma aproximação do tamanho da fonte e se está escrita em letras maiúsculas e/ou minúsculas. O indexador distribui esses *hits* em um conjunto de “barris”, criando um índice parcialmente ordenado. Ele analisa todos os links de cada página da web e armazena informações importantes sobre eles em um arquivo de âncoras.

<sup>49</sup> Texto original: “The idea of digitizing the entirety of the universe and making it work is something nobody was willing to tackle but lots of people knew needed to be done. They managed to get that together and bulldozed through the limitations. And with some luck, it is actually going to work.” (tradução livre)

<sup>50</sup> HTML é a linguagem de formatação das páginas web, criada por Tim Berners-Lee, considerado o pai da Web como a conhecemos.



Este arquivo contém informações suficientes para determinar para onde cada link aponta e de onde ele foi extraído, bem como o texto do link<sup>51</sup> (BRIN; PAGE, 2012)

A ideia de limitar a liberdade de tratamento computacional de informações disponibilizadas na web sempre foi bastante controversa. Em 1994, antes mesmo do Google ser idealizado, Martijn Koster, um engenheiro de computação holandês<sup>52</sup>, inicialmente pensando na diminuição de sobrecarga, nos servidores, gerados pelas aplicações que vasculham a internet para a criação dos índices de busca, criou o Protocolo de Exclusão de Robôs (*Robots Exclusion Protocol*), também conhecido como robot.txt, com o objetivo de dar aos administradores de sites (*webmasters*) o controle sobre quais dos seus conteúdos disponibilizados poderiam ser indexados pelos robôs (KOSTER, 2019). Apesar de amplamente utilizado, o robot.txt nunca se tornou um padrão oficial. Apenas em julho de 2019, na comemoração dos seus 25 anos, o seu pedido de oficialização foi encaminhado, pelo Google, ao Internet Engineering Task Force (IETF) (GOOGLE, 2019). Ao dar aos *webmasters* o controle sobre o que pode ou não ser indexado, o robot.txt (ou a meta tag *robots*) viabiliza uma solução técnica eficiente de proteção de conteúdo protegido por direitos autorais<sup>53</sup>, transferindo a responsabilidade do controle para o produtor e diminuindo a suscetibilidade do serviço quanto à utilização indevida de conteúdos de terceiros. Uma proteção técnica para potenciais problemas jurídicos decorrentes do desejo de concentrar toda a produção de conteúdo (inicialmente apenas em formato de texto) sob um controle centralizado.

Mas há também um outro aspecto relevante, além do desejo de capturar o máximo de conteúdo possível, produzido por outras pessoas. O objetivo, diferente de praticamente todos os outros serviços de disponibilização gratuita de conteúdo desenvolvidos até então, não era a reprodução pura e simples, mas a entrega de um resultado novo, derivado de um processamento computacional complexo. Havia uma **energia informacional potencial** naquele conjunto de páginas que poderia ser

<sup>51</sup> No original: "In Google, the web crawling (downloading of web pages) is done by several distributed crawlers. There is a URLserver that sends lists of URLs to be fetched to the crawlers. The web pages that are fetched are then sent to the storeserver. The storeserver then compresses and stores the web pages into a repository. Every web page has an associated ID number called a docID which is assigned whenever a new URL is parsed out of a web page. The indexing function is performed by the indexer and the sorter. The indexer performs a number of functions. It reads the repository, uncompresses the documents, and parses them. Each document is converted into a set of word occurrences called hits. The hits record the word, position in document, an approximation of font size, and capitalization. The indexer distributes these hits into a set of "barrels", creating a partially sorted forward index. The indexer performs another important function. It parses out all the links in every web page and stores important information about them in an anchors file. This file contains enough information to determine, where each link points from and to, and the text of the link." (tradução livre).

<sup>52</sup> Perfil pessoal no LinkedIn: <https://www.linkedin.com/in/martijnkoster/>  
Página pessoal: <https://www.greenhills.co.uk/> (Acesso em 06/01/2020)

<sup>53</sup> Atualmente existem diversas outras formas de proteção e de compatibilização do conteúdo protegido por direitos autorais com os sistemas de busca. Um deles é a possibilidade de indexação de conteúdo protegido por *paywalls* e fechados apenas para assinantes.

liberado, criando-se mais valor. Essa ideia também estava clara, desde o início do desenvolvimento do Google, como fica evidente na explicação dada por Larry Page sobre o PageRank, sistema de classificação de páginas que está na base do ranqueamento dos resultados de busca, na sua versão original (VISE; MALSEED, 2018):

“Toda vez que você cria um link”, Page disse ao público em silêncio, “você cria uma citação. Mas se você apenas tentar contar citações na Web, que é o que muitos mecanismos de pesquisa fazem, você terá problemas. A Web não é como literatura científica, porque qualquer pessoa pode produzir páginas da Web.”

“Uma maneira de pensar no PageRank”, ele explicou, “é um modelo de uso. Você tem um surfista aleatório na Web. É como um macaco, alguém que fica sentado e clica em links o dia todo e não tem inteligência alguma. Você pode argumentar que isso se aproxima do comportamento das pessoas na Web.” Page fez uma pausa, a platéia riu e ele continuou. “O PageRank está basicamente dizendo: se alguém aponta para você, você recebe uma fração da importância desse alguém. Digamos que alguém realmente importante aponte para você. Isso vale mais do que alguém que tem uma página da Web aleatória. Por exemplo, se o Yahoo apontar para você a partir da página inicial, isso é importante. Se você tiver apenas um link na página inicial do Yahoo, isso é muito bom. Você teve que pagar muito dinheiro a alguém ou sua página é muito boa. Se você tiver um link na minha página inicial, ninguém se importaria.” Page explicou como ele derivou sua receita para produzir resultados de pesquisa classificados. “Atribuímos números a essas páginas para corresponder aproximadamente à sua importância. A classificação da página é a soma de todas as coisas que apontam para ela”<sup>54</sup>

O número de classificação da página, gerado intrinsecamente pelo processamento do conteúdo do conjunto de páginas indexadas, submetidos a algoritmos complexos suportados por um poder computacional significativo, é genuinamente uma informação nova e de altíssimo valor. Por este motivo, precisa ser protegida. Ainda nos tempos de Stanford, Larry Page experimenta um sentimento contraditório, conforme relata Levy (2012):

Page tinha um conflito no que dizia respeito às informações. De um lado, ele se adequava perfeitamente à filosofia *hacker* de conhecimento compartilhado. Isso era parte do fundamento de seu projeto: tornar o conhecimento humano

<sup>54</sup> Texto original: “Every time you create a link,” Page told the hushed audience, “you’ve created a citation. But if you just try to count citations on the Web, which is what a lot of search engines do, you run into problems. The Web isn’t like scientific literature, because anybody can produce Web pages. “One way to think of PageRank,” he explained, “is it’s a usage model. You have a random [Web] surfer. It’s kind of like a monkey, just somebody who sits around and clicks links all day and doesn’t have any intelligence. You could argue that this kind of approximates people’s behavior on the Web.” Page paused, the audience chuckled, and he went on. “PageRank is basically saying, if somebody points to you, you get some fraction of the importance that they have. Let’s say somebody really important points to you. That’s worth more than someone who has a random Web page. For example, if Yahoo points to you from their homepage, that’s a big deal. If you just have one link on the Yahoo homepage, that’s pretty good. Either you had to pay someone a lot of money, or your page is pretty good. If you have a link on my homepage, nobody would pretty much care.” Page then explained how he derived his recipe for producing ranked search results. “We’ve assigned numbers to those pages to correspond roughly to their importance. The page’s ranking is the sum of all things pointing to it.” (tradução livre)

acessível, transformar o mundo em um lugar melhor. No entanto, ele também tinha uma forte vontade de proteger a propriedade da informação que tanto lutou para criar.

De modo similar ao que acontece com os dados pessoais, seguindo exatamente a descrição de Cohen (2019), na apropriação de conteúdo, ou seja, na face exposta do modelo de negócio dos serviços digitais disponibilizados gratuitamente, há uma fronteira clara, levantada por quem disponibiliza os serviços, entre dados em domínio público, acessíveis e de uso permitido, e informações protegidas por propriedade intelectual, em um sistema bastante sofisticado de geração de valor.

Ainda em relação à apropriação do conteúdo, há uma diferença substancial entre os serviços digitais, oferecidos gratuitamente, e os serviços de comunicação *broadcast*. O rádio e a TV foram construídos dentro de um rígido regime de preservação dos direitos autorais, essencialmente porque ou o conteúdo era diretamente desenvolvido pelo veículo ou era comprado de um terceiro e disponibilizado preservando exatamente a sua estrutura, com baixíssimas margens para adequação ou edição. Outro ponto relevante da diferença entre os veículos *broadcast* e os serviços digitais está na origem do conteúdo. Enquanto rádios e TVs basearam sua distribuição quase que exclusivamente em produções profissionais, com baixíssimo índice de participação dos usuários, pela própria natureza do meio, que sozinho não permite interação, os sistemas digitais reempacotam e distribuem conteúdo profissional, mas quase de modo indistinto, empacota e distribui conteúdo de pessoas comuns, que são criados não de forma profissional, mas pelo simples fato de desejarem compartilhá-lo, seja com um grupo restrito, seja com o maior número possível de pessoas.

O lançamento do Google News, em 2002, exemplifica bem o modo como provedores de serviços digitais gratuitos encaram os conteúdos de terceiros, mesmo aqueles produzidos profissionalmente. Idealizado por Krishna Bharat e tendo como gerente Marissa Mayer, posteriormente vice-Presidente do Google e presidente do Yahoo, o Google News é um agregador de notícias produzidas por veículos de comunicação. Como lembram Vise e Malseed (2018), “O que dava ao Google direito de republicar notícias produzidas por várias companhias de mídia em seu próprio website? Nada, na realidade”<sup>55</sup>, afinal, sob o seu ponto de vista, o objetivo não era adquirir as notícias para republicá-las, o que significaria a necessidade de licenciar e pagar os provedores de conteúdo. A ideia era tornar-se um ponto de acesso que levaria os usuários para os conteúdos mais relevantes mais rapidamente.

Mas nem todos os veículos de imprensa ficaram felizes com o uso, sem remuneração, de seus conteúdos por uma grande companhia, para disponibilização de um serviço sobre o qual não aferiam nenhum ganho. Em 2014, a Espanha aprovou uma

<sup>55</sup> No original: “What gave Google the right to republish news produced by various media companies on its own Web site? Nothing, really.” (tradução livre)

nova lei de direitos autorais que previa a necessidade de pagamento, pelos concentradores de notícias online, pelos links e trechos de notícias produzidas pelos veículos de comunicação locais disponibilizados em seus serviços, com multas que podem chegar a até 600 mil euros. Como consequência, o Google desativou a versão local do Google News, no mês de dezembro do mesmo ano, dias antes da legislação entrar em vigor (RUSHE, 0014).

Em abril de 2019, a União Europeia aprovou a Diretiva 2019/790, relativa aos direitos de autor e direitos conexos no mercado único digital que, em seu artigo 15, garante aos veículos a preservação de seus direitos quanto ao uso de suas publicações por prestadores de serviços digitais, excetuando os casos de utilização exclusiva de *hiperlinks* ou de excertos muito curtos das publicações (EUROPA, 2019).

Todo esse revés não ficou sem resposta. Em março de 2018, o Google lançou o Google News Initiative, um esforço para, segundo a companhia, “ajudar o jornalismo a prosperar na era digital”<sup>56</sup> (SCHINDLER, 2018). Este tipo de ação pode ser um indicativo de que um reequilíbrio de forças talvez não passe pela remuneração direta dos veículos pelo Google, mas pode seguir um curso parecido com o que já é feito com os anunciantes.

Na relação com os anunciantes, além de demonstrar que, comparativamente, anunciar nos serviços Google gera resultados superiores, a companhia também disponibiliza, gratuitamente ou a preços relativamente acessíveis, serviços que, fazendo tratamento de dados pessoais, auxiliam o anunciante a melhorar seu desempenho, não apenas quanto à eficácia dos anúncios, mas no aumento efetivo de conversões, sejam vendas ou outros objetivos de marketing pretendidos pelo cliente. Esse é o caso clássico do Google Analytics. O mesmo caminho parece estar sendo seguido na relação com os publishers. Em setembro de 2019, Richard Gingras, Vice-Presidente de Notícias, do Google, publicou em um post do blog da companhia:

No mundo dos veículos impressos, os veículos pagam bancas para exibir seus jornais e revistas, para que os leitores possam descobri-los. O Google oferece esse benefício aos editores sem nenhum custo. Isso cria valor real: somente na Europa, as pessoas clicam nos conteúdos de notícias que o Google veicula mais de 8 bilhões de vezes por mês - são 3.000 cliques por segundo que direcionamos para os sites dos próprios veículos. Para grandes veículos, um estudo da Deloitte coloca o valor de cada clique entre 4-6 centavos de euro.

Além do tráfego que enviamos aos veículos, continuamos investindo e agregando valor ao setor jornalístico de outras maneiras. As tecnologias de publicidade do Google são usadas por muitos sites, incluindo veículos de imprensa, nos quais os veículos retêm a grande maioria da receita publicitária. Em 2018, o Google enviou mais de 14 bilhões de dólares para veículos de todo o mundo.

Nossa Google News Initiative está investindo US\$ 300 milhões para ajudar os veículos de todo o mundo a desenvolver novos produtos e modelos de negócios que se ajustem aos diferentes mercados de publicação que a Inter-

<sup>56</sup> No original: “help journalism thrive in the digital age” (tradução livre)

net viabiliza. E continuamos a fazer melhorias para conectar as pessoas às notícias a partir de nossos produtos<sup>57</sup> (GINGRAS, 2019)

Como na relação com os anunciantes, onde parte do *pagamento* pela disponibilização das ferramentas de otimização se dá pela expansão da capacidade de coleta de dados pessoais a partir de *embed codes*, também no caso dos *publishers* os dados pessoais poderão funcionar como uma conveniente contrapartida.

### 2.3.2 Nossa vida como conteúdo

A mesma lógica de apropriação de conteúdo acontece nas redes sociais, só que desta vez o conteúdo é cedido de modo voluntário. Importante notar que a distinção deste cenário para o dos outros serviços é a **voluntariedade**, não o caráter do conteúdo em si, que pode ser tanto pessoal quanto profissional. Mais uma vez, estas duas categorias se misturam e são processadas, convenientemente, pelos serviços, tanto no sentido de aumentar a sua atratividade, sob o ponto de vista dos usuários, quanto para aumentar sua eficácia na geração de receita, massivamente por meio de leilões de publicidade online.

O cientista da computação e compositor Jaron Lanier, um dos precursores da realidade aumentada, baseado nas robôs femininas forjadas por Hefesto, descritas por Homero na *Ilíada*, cunhou o termo *Siren Server* (Servidor Sereia), para descrever um grande computador ou uma coleção coordenada de computadores em rede, capaz de

coletar dados da rede, geralmente sem ter que pagar por isso. Os dados são analisados usando os computadores mais poderosos disponíveis, operados pelos melhores técnicos disponíveis. Os resultados da análise são mantidos em segredo, mas são usados para manipular o resto do mundo para gerar vantagem<sup>58</sup> (LANIER, 2013).

Como as sereias mitológicas, mesmo com os avisos de alerta os marinheiros que navegam pelas redes geralmente sucumbem. Elas seriam primas de outro ser (na realidade, algo), o Demônio de Maxwell, descrito por James Clerk Maxwell, físico

<sup>57</sup> Texto original: "In the world of print, publishers pay newsstands to display their newspapers and magazines so readers can discover them. Google provides this benefit to publishers at no cost. This creates real value: In Europe alone, people click on the news content Google links to more than 8 billion times a month—that's 3,000 clicks per second we drive to publishers' own websites. For large news publishers, a study by Deloitte puts the value of each click between 4-6 euro cents. Beyond the traffic we send to publishers, we continue to invest in and provide value to the news industry in other ways. Google's advertising technologies are used by many websites, including news publishers, where publishers retain the vast majority of the ad revenue. In 2018, Google sent more than 14 billion dollars to publishers around the world. Our Google News Initiative is investing \$300 million to help news publishers around the world develop new products and business models that fit the different publishing marketplace the Internet has enabled. And we continue to make improvements to connect people with news from our products." (tradução livre)

<sup>58</sup> Texto original: "gather data from the network, often without having to pay for it. The data is analyzed using the most powerful available computers, run by the very best available technical people. The results of the analysis are kept secret, but are used to manipulate the rest of the world to advantage." (tradução livre)

britânico que estabeleceu a formulação matemática dos campos magnéticos, que seria capaz de violar a segunda lei da termodinâmica. A ideia do Demônio de Maxwell está ligada aos limites físicos da computação mecânica (PASSOS JR., 2017). Para Lanier, todo bit de um computador é um aspirante a Demônio de Maxwell que separa, por um tempo, os estados '1' e '0' (o demônio original separava moléculas quentes e frias), mas a um determinado custo. Da mesma forma, Servidores Sereia podem separar pessoas conectadas, a partir da análise dos seus dados, selecionando-as e abrindo ou fechando oportunidades para elas, a critério da própria Sereia.

Um ponto relevante do pensamento de Lanier refere-se ao fato de que a Sereia encanta e pode destruir até mesmo quem a controla, já que os resultados e a mitigação de risco de curto prazo têm potencial de geração de efeitos negativos severos de longo prazo, decorrentes do impacto social do uso dessas tecnologias. E apresenta um exemplo didático, ligado à indústria de seguros:

Uma *Siren Server* pode permitir que apenas aqueles cujo custo para segurar seja baixo atravessem uma porta (se tornem segurados) de modo a criar uma companhia de seguros sobrenaturalmente ideal e de baixo risco. Tal esquema permitiria que pessoas de alto risco passassem por um caminho, e pessoas de baixo risco passassem pelo outro, a fim de implementar uma máquina de movimento perpétuo falso em uma sociedade humana. No entanto, os não segurados não deixariam de existir; em vez disso, aumentariam o custo do sistema como um todo, incluindo as pessoas que executam o *Siren Server*. Uma ilusão de curto prazo de redução de risco levaria a um aumento de risco a longo prazo<sup>59</sup>.

Agora, do ponto de vista individual, o que leva uma pessoa a cair no canto da sereia das redes sociais? O que as leva a compartilhar, com um grupo reduzido ou com todos, um volume expressivo de informações pessoais, momentos de vida, expressões de pensamento, em um formato de linha do tempo, intermediados por serviços que empacotam esses conteúdos e os disponibilizam em serviços que, na realidade, são pagos por empresas e organizações que enxergam essas mesmas pessoas como consumidores, mesmo que o que esteja *a venda* não seja um produto ou serviço de consumo?

A ideia de uma sociedade de consumidores, trazida por Zygmunt Bauman, onde as pessoas ocupam uma posição dupla - simultaneamente são mercadorias disponíveis no mercado e agentes de marketing desta mercadoria - pode ajudar a compreender esse comportamento.

<sup>59</sup> No original: "A Siren Server might allow only those who would be cheap to insure through a doorway (to become insured) in order to make a supernaturally ideal, low-risk insurance company. Such a scheme would let high-risk people pass one way, and low-risk ones pass the other way, in order to implement a phony perpetual motion machine out of a human society. However, the uninsured would not cease to exist; rather, they would instead add to the cost of the whole system, which includes the people who run the Siren Server. A short-term illusion of risk reduction would actually lead to increased risk in the longer term." (tradução livre)

Apesar de aparentemente paradoxal, este fenômeno configura-se como verdadeiro simulacro, onde o “fetichismo da subjetividade”, para utilizar uma expressão citada por Baudrillard, não esconde uma outra verdade, mas esconde, sim, que na realidade não existe. Como todo simulacro, o fetichismo da subjetividade e a ultra valorização do indivíduo são verdadeiros. O autor não deixa dúvidas quanto a isso quando, por exemplo, estabelece:

Como compradores, fomos adequadamente preparados pelos gerentes de marketing e redatores publicitários a desempenhar o papel de sujeito – um faz de conta que se experimenta como verdade viva; um papel desempenhado como “vida real”, mas que com o passar do tempo afasta esta vida real, despindo-a, nesse percurso, de todas as chances de retorno.

Ao apresentar esta ideia de *produtização* humana, encoberta pela exaltação da escolha, fundada no fetichismo da subjetividade, Bauman revela o segredo mais bem guardado da sociedade de consumidores.

Outro aspecto relevante da sociedade de consumidores, segundo Bauman, é a necessidade de satisfação imediata em substituição da ideia de riqueza durável, que marca a modernidade clássica, muito bem detalhada por Veblen. Nasce, então, o conceito de tempo pontuado ou pontilhista, formado por um conjunto de “instantes eternos”. Impossível não fazer uma associação deste conceito com o que se observa em redes sociais digitais baseadas em fotos, como é o caso do Instagram. O conceito do produto funda-se nesta ideia: a captura, no menor intervalo de tempo possível, de instantes de felicidade que precisam ser compartilhados com todos. Como bem destaca Bauman, “a sociedade de consumidores é avaliada, para o bem ou para o mal, pela felicidade de seus membros”.

Assim, fecha-se o ciclo. Nesta estrutura, os membros da sociedade são, eles próprios, mercadorias de consumo. Mais uma vez, é impossível não fazer uma correlação entre o pensamento de Bauman e a ‘engenharia’ das redes sociais. Observamos o comportamento dos profissionais-mercadoria em redes sociais profissionais, como o LinkedIn, ou dos “amigos-mercadoria” em redes sociais genéricas, como é o caso do Facebook, verdadeiros *displays* rolantes, dispostos em *timeline*. Inegável que, ao olhar estas estruturas levando-se em consideração este mercado de consumidores, o próprio termo feed (alimentar) passa a ter uma conotação de consumo.

O efeito de rede também ajuda a entender o fenômeno. Nas redes sociais esse efeito é evidente e explica, em grande medida, o crescimento de plataformas como o Facebook. A plataforma atrai mais usuários porque já possui um grande volume de usuários. Dando contornos mais econômicos, segundo a definição de Shapiro e Varian (1999), já em 1998, ou seja, muito antes do surgimento das redes sociais digitais:

Para muitas tecnologias da informação, os consumidores se beneficiam do uso de um formato ou sistema popular. Quando o valor de um produto, para um usuário, depende de quantos outros usuários existem, os economistas

dizem que este produto exibe externalidades ou *efeitos de rede*. (...) As tecnologias sujeitas a fortes efeitos de rede tendem a exibir longo *lead time*<sup>60</sup> seguido de crescimento explosivo. O padrão resulta de feedback positivo: à medida que a base instalada de usuários cresce, mais e mais usuários acham que a adoção vale a pena. Eventualmente, o produto atinge massa crítica e assume o mercado. (...) Mas as externalidades de rede não se limitam às redes de comunicação. Eles também são poderosos em redes "virtuais"(...) Como essas redes virtuais de usuários compatíveis geram externalidades de rede, os sistemas populares de hardware e software desfrutam de uma vantagem competitiva significativa em relação aos sistemas menos populares. (...) O desafio chave é obter massa crítica. Uma vez que você tem uma base de clientes grande o suficiente, o mercado será construído por si mesmo. Porém, ter uma tecnologia superior não é suficiente. Você precisa empregar ferramentas de marketing, tais como preço de penetração para dar início ao feedback positivo. As empresas que melhor entenderem sistemas de informação e produtos complementares terão melhores posicionamentos para se moverem rapidamente e agressivamente.<sup>61</sup>

Lanier divide o efeito de rede em duas categorias: de recompensa e de punição, sendo que as *Siren Servers*, como as redes sociais, por exemplo, ganham dominância a partir de efeitos de rede de recompensa, mas mantêm a dominância por meio de efeitos de rede de punição. Isso significa que, na entrada, o consumidor (esse efeito se aplica tanto para o usuário quanto para o anunciante) observa um ganho efetivo, mas se desejar sair deve absorver uma perda. O autor dá o seguinte exemplo, relativo ao Facebook:

Se uma grande quantidade de criatividade pessoal e experiência de vida foi adicionada ao site, é difícil desistir de tudo isso. Mesmo se você capturar tudo o que você carregou no site, não poderá salvá-lo no contexto de interações com outras pessoas. Você precisa perder uma parte de si mesmo para deixar o Facebook depois de se tornar um usuário ávido. Se você sair, será difícil para algumas pessoas entrar em contato com você. Você estaria disposto a correr o risco de separar uma parte do contexto de sua própria vida para se libertar de um Siren Server que lhe interessa?<sup>62</sup> (LANIER, 2013)

<sup>60</sup> Nota: com o efeito exponencial do desenvolvimento de novas tecnologias e novos serviços digitais, o *lead time* vem caindo drasticamente.

<sup>61</sup> No original: "For many information technologies, consumers benefit from using a popular format or system. When the value of a product to one user depends on how many other users there are, economists say that this product exhibits network externalities, or network effects. (...) Technologies subject to strong network effects tend to exhibit long lead times followed by explosive growth. The pattern results from positive feedback: as the installed base of users grows, more and more users find adoption worthwhile. Eventually, the product achieves critical mass and takes over the market. (...) But network externalities are not confined to communications networks. They are also powerful in "virtual" networks (...) Because these virtual networks of compatible users generate network externalities, popular hardware and software systems enjoy a significant competitive advantage over less popular systems. (...) However, having a superior technology is not enough. You may need to employ marketing tools such as penetration pricing to ignite the positive feedback. The company that best understands information systems and complementary products will be best positioned to move rapidly and aggressively."(tradução livre)

<sup>62</sup> No original: "If a great deal of personal creativity and life experience has been added to the site, it's hard to give all that up. Even if you capture every little thing you had uploaded, you can't save it in the context of interactions with other people. You have to lose a part of yourself to leave Facebook once you become an avid user. If you leave, it will become difficult for some people to contact you at all. Would you ever be willing to take the risk to sever a part of your own life's context in order to



Tentando aumentar a esfera de direitos dos titulares de dados e mitigar, em alguma medida, a tendência monopolista dos serviços digitais, legislações de proteção de dados estabelecem o direito a portabilidade dos dados pessoais. Na LGPD, o inciso V, do art. 18, estabelece a possibilidade de “portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial”. Mesmo considerando que todas as questões técnicas relacionadas à portabilidade sejam vencidas, isso quer dizer, que um fornecedor tenha capacidade (e vontade) de exportar os dados pessoais em um formato que possa ser processado adequadamente por outro, ou ainda, em um cenário ideal e, por isso, distante da realidade, seja possível o estabelecimento de um padrão de portabilidade, os efeitos de rede punitivos não desaparecem. A exportação dos dados pessoais, para portabilidade, não exporta o contexto. Mesmo que todos os usuários exportem seus dados e os carreguem em outra rede, a simples possibilidade de existir alguém, ou um grupo de pessoas, que se recuse a fazer uma migração de serviços impede uma exportação, mesmo que hipotética, do contexto de uma plataforma a outra, pela simples necessidade de preservação dos direitos relativos aos dados pessoais daqueles que pretendem se manter na plataforma original. Não há, portanto, solução individual para algo que nasce e se forma como rede. E, neste ponto, as legislações de proteção de dados, como a LGPD e a GDPR falham, pelo mesmo motivo que falham em diversos outros pontos: a centralidade na proteção dos dados pessoais, sem observar os outros aspectos manejados pelos serviços digitais gratuitos, não é suficiente para garantir um nível adequado da proteção à personalidade.

### 3 CONSUMIDOR. MATÉRIA-PRIMA. PRODUTO.

Como visto no Primeiro Capítulo, plataformas digitais disponibilizadas sem contrapartida financeira por parte dos usuários articulam, como meios de produção: (a) alta capacidade de processamento de informação (poder computacional e *softwares* eficientes), ou seja, capital; (b) dados pessoais e conteúdo dos outros, como matéria prima, e (c) alocação de tempo dos usuários, em certo sentido como mão de obra não remunerada, para a criação dos espaços publicitários que serão leiloados entre os anunciantes. Como resultado deste processo produtivo, do lado gratuito, a plataforma entrega conteúdo relevante para os usuários, considerando-se relevante a informação mais alinhada aos seus interesses, no contexto de uso da aplicação. Já do lado pago, entrega anúncios a usuários mais propensos a converterem aquela exposição à mensagem publicitária em uma ação efetiva em favor do anunciante. Imediatamente, em um acesso a um ambiente digital (*landing page*, site, e-commerce etc) do anunciante e, de forma mediata, em um resultado mais contundente, como a realização de uma venda. Tudo isso, garantindo-se o rastreamento, ao menos nas ações realizadas na web, e, em alguns casos, por aplicações fornecidas pela própria plataforma.

Essa arquitetura de aplicação coloca o usuário em três posições distintas. A primeira, óbvia e direta, de consumidor de um serviço digital que lhe é oferecido sem a necessidade de uma contrapartida financeira, pecuniária. Na primeira seção deste capítulo, os serviços serão analisados sob este ponto de vista, como plataformas de dois lados ou multilaterais, seu potencial de diminuição de bem estar para os usuários, decorrentes do abuso de posição dominante, gerado pelo alto poder de mercado e sua tendência ao monopólio.

Em seguida, passa-se à análise da posição do usuário como fornecedor da matéria-prima, essencialmente dados pessoais, necessária para que a plataforma possa oferecer, de modo eficiente, seus serviços para os clientes 'do outro lado': os anunciantes. Inicia-se pela dupla caracterização dos dados pessoais, como parte essencial da personalidade e, ao mesmo tempo, um ativo economicamente apreciável cada vez mais valioso. Em seguida, parte-se para algumas considerações relevantes sobre a proteção constitucional dos dados pessoais, a partir de uma visão ampliada, não focada apenas na necessidade de controle das atividades de tratamento, mas também levando em consideração os resultados gerados por essas atividades.

Finaliza o capítulo a abordagem da terceira posição concomitante ocupada pelos usuários das plataformas: o de alvo da publicidade direcionada, viabilizada pelas plataformas. Ou seja, a posição de produto. A partir do pressuposto de que os dados, vistos como meios de produção (matéria prima), geram retornos decrescentes, sugerida por Varian (2019), evidencia-se o caminho que leva a *economia do encontro* a desencadear a *economia da vigilância*.

### 3.1 GRATUIDADE, CONCENTRAÇÃO DE PODER E O MERCADO DE UM

No Tampa Stadium, na Flórida, no dia 22 de janeiro, Los Angeles Raiders e Washington Redskins decidiram o Super Bowl XVIII. Os Redskins, vendedores da temporada anterior, buscavam seu segundo triunfo<sup>1</sup>. Já os Raiders queriam faturar seu terceiro título.

O time de Los Angeles foi o grande vencedor da noite, batendo o Redskins por 38 a 9, mas este não foi o fato mais marcante da final do campeonato de futebol americano de 1.984. Aproveitando a *coincidência* de datas, a Apple lançou seu computador pessoal Macintosh, no intervalo desse jogo, com um comercial antológico, dirigido por Ridley Scott, que pouco antes havia dirigido Blade Runner, um clássico da ficção científica no cinema, adaptado da obra *Androides sonham com ovelhas elétricas?* (*Do Androids Dream of Electric Sheep?*), de Philip K. Dick.

Em sessenta segundos, uma visão sombria do futuro é contrastada com uma mulher que corre por um corredor até chegar a um salão onde uma multidão catatônica ouvia as palavras do Grande Irmão em uma imensa tela. Ao chegar lá, ela lança um imenso martelo contra a imagem do Grande Irmão. Após uma grande explosão, uma mensagem corre pela tela: “Em 24 de janeiro, a Apple lançará o Macintosh. E você verá por que 1984 não será como ‘1984’”<sup>2</sup>. Depois deste dia, o filme entrou para a história e nunca mais foi veiculado.

Como descreve Lee Clow (2014), um dos diretores de criação da agência, que participou diretamente da concepção do comercial, o Grande Irmão representava “o controle da tecnologia por poucos”. Muitos viram uma relação direta entre o Grande Irmão e a IBM, tanto pelos contornos de mercado à época quanto pelo tom *azulado* do filme. Apesar de não confirmar que esta tinha sido uma intensão previamente pensada, Clow reconhece que a associação funcionou na prática.

A apropriação do cenário distópico descrito por Orwell, em 1984, acontece desde o lançamento da obra, em diversas esferas, e o uso comercial dos seus conceitos é apenas uma delas. Esse futuro projetado parece-nos assustadoramente real, mas não deixa de ser irônico o fato de que, hoje, o controle e o poder excessivos nas mãos de gigantes da tecnologia, como denunciava o filme, continuam sendo ameaças relevantes, só que agora a Apple faz parte desse grupo.

De todas as associações possíveis entre o mundo de Orwell e o nosso mundo, há uma característica especialmente relevante para a abordagem sobre serviços digitais disponibilizados gratuitamente: a novafala. Mesmos C. S. Lewis (2018), crítico contumaz de *1984*, que achava o livro muito inferior a *A Revolução dos Bichos*, ressal-

<sup>1</sup> Além do Super Bowl XVII, o time havia conquistado outros dois campeonatos da NFL, em 1937 e 1942, antes de existir Super Bowl. Também foram campeões das edições XXII (1987) e XXVI (1991)

<sup>2</sup> No original: “On January 24th, Apple Computer will introduce Macintosh. And you’ll see why 1984 won’t be like ‘1984’” (tradução deste mestrando)

tou a importância do “magnífico, e felizmente destacável, apêndice sobre a *Novafala*”<sup>3</sup>.

Uma nuance discursiva relevante da *novafala* é a utilização de eufemismos para inverter a polaridade dos sentidos. Nos exemplos clássicos, o Ministério da Paz (Minipaz) é responsável pela guerra; o Ministério do Amor (Miniamor), responsável pela lei e a ordem, fazia a “controle do ódio” e o Ministério da Verdade (Miniver) controla a opinião e cerceia a liberdade de expressão. Na estrutura da *novafala*, estas são as palavras do Vocabulário B, criadas com propósitos políticos e que nunca eram neutras. Como exposto no próprio apêndice do livro, ao tratar dessa categoria de vocabulário: “Muitas não passavam de eufemismos. O significado de palavras como *campofolia* (campo de trabalhos forçados) e *Minipaz* (Ministério da Paz, isto é, Ministério da Guerra), era quase exatamente o inverso do que pareciam significar” (ORWELL, 2019).

A utilização deste mecanismo na *novafala* foi, no caso de Orwell, uma transposição, para a ficção, de seu posicionamento na vida real, onde denunciou esta mesma aplicação eufemística, que promove a inversão de sentidos, no discurso político:

Em nosso tempo, o discurso e a escrita política são, em grande medida, a defesa do indefensável. Podem-se defender coisas como a continuação do domínio britânico na Índia, os expurgos e as deportações russas, as bombas atômicas jogadas sobre o Japão, mas somente com argumentos que são brutais demais para a maioria das pessoas e que não estão de acordo com os objetivos declarados dos partidos políticos. Desse modo, a linguagem política precisa consistir, em larga medida, em eufemismos, argumentos circulares e pura imprecisão nebulosa. Aldeias indefesas são bombardeadas por aviões, os habitantes são expulsos para o campo, o gado é metralhado, as cabanas incendiadas por bombas incendiárias: isso se chama pacificação. Milhões de camponeses têm suas fazendas roubadas e são mandados para a estrada com não mais do que aquilo que podem carregar consigo: isso se chama transferência da população ou retificação de fronteiras. Pessoas ficam presas durante anos, sem julgamento, ou são fuziladas na nuca, ou são mandadas para morrer de escorbuto em acampamentos de lenhadores no Ártico: isso se chama eliminação de elementos não confiáveis. Essa fraseologia é necessária se quisermos nomear coisas sem evocar imagens mentais delas. (ORWELL, 2009).

A ideia de gratuitos, para designar o tipo de modelo de negócio onde os serviços são pagos com dados pessoais e alocação de tempo dos usuários, aplica essa mesma técnica de eufemismos denunciada por Orwell. Não apenas para dar contornos positivos para um sistema de apropriação de bens alheios, mas também como instrumento de afirmação. Isso fica claro, por exemplo, na entrevista concedida por Eric Smitch, então CEO do Google, logo após ser convocado para uma audiência no Congresso Americano: “Então, somos levados à frente do Congresso por desenvolver um produto gratuito, que atende a um bilhão de pessoas. OK? Quero dizer, não sei como dizer isso de maneira mais clara. Não é como se tivéssemos aumentado os preços. Poderíamos baixar os preços de grátis para... menos que grátis?”<sup>4</sup>.

<sup>3</sup> Uma nota relevante: “felizmente destacável” é uma expressão utilizada por Lewis e não reflete o pensamento do autor deste trabalho sobre a obra ‘1984’.

<sup>4</sup> Texto original: “So we get hauled in front of the Congress for developing a product that’s free, that

O mesmo se observa nos próprios termos de uso das plataformas (grifos nossos).

No Facebook (2019),

*Não cobramos pelo uso do Facebook ou de outros produtos e serviços cobertos pelos Termos. Em vez disso, empresas e organizações nos pagam para lhe mostrar anúncios de seus produtos e serviços. Quando você usa nossos Produtos, concorda que podemos mostrar anúncios que consideramos relevantes para você e seus interesses. Usamos seus dados pessoais para ajudar a determinar quais anúncios mostrar.*

Já no Google (2017),

*Nossos sistemas automatizados analisam o seu conteúdo (incluindo e-mails) para fornecer recursos de produtos pessoalmente relevantes para você, como resultados de pesquisa customizados, propagandas personalizadas e detecção de spam e malware. Essa análise ocorre à medida que o conteúdo é enviado e recebido, e quando ele é armazenado.*

Nesta seção, aborda-se as estruturas de funcionamento das plataformas que vão além da utilização dos dados pessoais para a melhoria da experiência do usuário, expondo as engrenagens que transformam, com grande poder computacional, dados pessoais e tempo em uma lucrativa máquina de segmentação, com grande potencial de vigilância e influência.

Ao contrário do que parecia estar à vista de Orwell como projeção de um futuro não muito distante, o mais aterrorizante controle potencial das plataformas disponibilizadas gratuitamente não é apenas a massificação do pensamento. O sucesso destas plataformas, em grande medida, está em identificar e fazer com que os usuários se sintam, orgulhosos, satisfeitos e sem medo, como uma *minoria de um*. Numa dicção econômica, um mercado de um.

### 3.1.1 A economia da privacidade

A todo momento, em nossa vida diária, realizamos transações envolvendo dados pessoais. Ao utilizar uma aplicação de mapas, implicitamente vendemos nossos dados de localização; vendemos informações com nossos interesses imediatos quando utilizamos um mecanismo de busca; vendemos nossa teia de relacionamentos, nossa imagem nas fotos, nossos interesses e nosso estado emocional quando utilizamos uma rede social.

Até os nossos metadados são transacionados. Pegando como exemplo o WhatsApp, se o usuário tirar um tempinho - o diminutivo aqui tem uma conotação irônica - para ler os termos de uso e a política de privacidade da aplicação, verá escrito (versão de 19 de dezembro de 2019, com grifo nosso):

---

serves a billion people. OK? I mean, I don't know how to say it any clearer. It's not like we raised prices. We could lower prices from free to... lower than free?" (tradução deste mestrando)

Passamos a fazer parte da família de empresas do Facebook em 2014. Como parte desta família, o WhatsApp recebe e compartilha dados com os demais membros. Podemos usar os dados fornecidos por eles e eles podem usar os dados compartilhados por nós para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços e as ofertas deles. Isso inclui a ajuda no aprimoramento dos sistemas de infraestrutura e entrega, a compreensão de como nossos Serviços ou os serviços deles são usados, a proteção dos sistemas e o combate a spam, abuso ou atividades que violem o uso lícito destes. *O Facebook e outras empresas do mesmo grupo também podem usar dados do WhatsApp para fazer sugestões (por exemplo, de amigos, de contatos ou de conteúdo interessante) e mostrar ofertas e anúncios relevantes.* No entanto, *suas mensagens do WhatsApp permanecem privadas e não serão compartilhadas no Facebook para que outros vejam.* Na verdade, o Facebook não usará suas mensagens do WhatsApp por qualquer motivo que não seja nos auxiliar na operação e na execução dos Serviços. (WHATSAPP INC, 2019)

Uma pergunta pode ser feita, ao ler o trecho da Política de Privacidade: como é possível fazer sugestões e mostrar ofertas e anúncios relevantes sem ter acesso às mensagens? Pelos metadados. Em uma definição bastante concisa, metadados são aquelas informações que não são os dados propriamente ditos, mas que os descrevem ou os acompanham. O poder desse tipo descritivo de dado, do ponto de vista de rastreabilidade de hábitos ou ações dos usuários, pode ser visualizado a partir de um exemplo.

Imagine uma pessoa de hábito alimentar vegano. Semanalmente, ela faz pedidos de comida vegana em uma pequena loja, que prepara os alimentos de forma artesanal, onde a dona da loja é quem faz a comida, atende os clientes e também faz as entregas. Os pedidos são feitos pelo WhatsApp, em uma comunicação direta e criptografada entre a cliente e a dona da loja, ou seja, nem o WhatsApp sabe qual o teor dessa conversa, mas tem acesso a metadados, como o fato de que estas pessoas estão conversando, que a conversa é baseada apenas em troca de mensagens de texto e que sempre ocorrem com uma frequência específica. Esta nossa personagem vegana, como quase todos atualmente, possui um perfil no Facebook e associou a este perfil seu telefone celular. Da mesma forma, a dona da loja possui uma página nesta rede social e associou o seu celular pessoal à página da loja. Temos um cenário, aqui, onde os dados disponíveis ao fornecedor de serviços digitais podem ser cruzados com metadados para que este consiga saber mais sobre as pessoas do que elas dizem diretamente. No caso do nosso exemplo, um sistema de inteligência artificial conseguiria analisar a frequência, o tipo e o tamanho da comunicação entre a pessoa vegana e a dona da loja e, sabendo que o telefone desta última está associado a uma loja de produtos veganos, pode inferir que nossa personagem faz pedidos pelo sistema de mensagens em datas específicas. A partir desta simples inferência, o Facebook pode começar a “entregar” publicidade de lojas de produtos veganos para a nossa personagem em momentos muito próximos daqueles em que ela faz seus pedidos, aumentando a chance de conversão do anúncio e influenciando os hábitos de con-

sumo de nossa personagem vegana, a partir de dados que ela não disse ao Facebook. Essa é uma das formas como a concentração dos serviços digitais pode vulnerar a privacidade, pelo cruzamento de dados conhecidos, diretamente disponibilizados pelos usuários, e informações inferidas a partir do cruzamento de metadados, muitas vezes vindos de outras aplicações de um mesmo fornecedor.

Esse caso hipotético demonstra uma situação bastante comum nas transações envolvendo dados pessoais: muitas vezes, o usuário não tem consciência plena dos diversos modos de coleta e categorias dos dados pessoais, muito menos consegue visualizar o tipo de utilização realizada pelos fornecedores, o que impede, na prática, um consentimento livre e informado sobre esta utilização. O excerto do trecho dos Termos de Uso do WhatsApp, quando trata do compartilhamento de dados entre empresas da *família Facebook*, não permite ao usuário médio, que não possui conhecimento técnico ou tenha estudado especificamente o assunto, inferir o uso descrito neste exemplo.

Isso acontece porque, como explicam Acquisti, Taylor e Wagman (2016), para os provedores de serviço, o comércio de dados (*data trading*) é a essência da transação, enquanto para o usuário ele é secundário e, muitas vezes, invisível, encoberto por uma transação muito mais proeminente, como a troca de mensagens com alguém, a apresentação de uma foto a um grupo de amigos ou a tentativa de não errar uma curva enquanto dirige um carro, permanecendo na rota traçada pelo aplicativo.

A economia da privacidade é uma subárea da economia da informação que estuda, do ponto de vista econômico, este tipo de transação. Para isso, parte de uma premissa básica: “a proteção ou divulgação de dados pessoais podem gerar *trade-offs* com dimensões econômicas tangíveis<sup>5</sup>.” (ACQUISTI; TAYLOR; WAGMAN, 2016).

Partindo dessa premissa, privacidade não deve ser entendida como o oposto do compartilhamento, mas como controle sobre o que se compartilha ou não, em uma visão muito próxima daquela defendida, no âmbito jurídico, por Rodotà (2008), que definiu privacidade como “o direito de manter o controle sobre as próprias informações e *determinar as modalidades de construção da própria esfera privada*.” (grifo no original).

Visto no quadro geral, econômico e jurídico, deve-se levar em conta que abordagens baseadas no mercado e abordagens regulatórias não são mutuamente excludentes, mas as suas articulações conjuntas formam um espectro onde, em uma extremidade há um regime sem nenhuma regulação e a proteção dos dados pessoais dependeria exclusivamente das regras de mercado. No outro ponto do espectro, a regulação definiria estritamente as condições de proteção de dados pessoais e os limites de uso. Essa ideia abre espaço para entender a privacidade como uma modulação entre regulação e forças de mercado, na busca da melhor conciliação de interesses (ACQUISTI; TAYLOR; WAGMAN, 2016).

<sup>5</sup> Original: “the protection and disclosure of personal data are likely to generate trade-offs with tangible economic dimensions” (tradução deste mestrando)

Os mesmos autores também identificam cinco características peculiares das transações envolvendo dados pessoais, quando analisados como bens econômicos:

**a. Quando compartilhados, dados pessoais possuem características de bens públicos**

Em uma definição breve, bens públicos puros são produtos ou serviços que são indivisíveis ou não excludentes. Isso significa que o bem pode ser consumido por muitas pessoas e uma vez disponível, o custo marginal de incremento de consumo é zero. Neste caso, em um sistema de concorrência perfeita, o preço também é igual a zero. (TRUETT; TRUETT, 2004) Os dados pessoais, em regra, são não rivais e não excludentes, características ligadas a bens públicos. Como os custos de distribuição (duplicação e transferência) são próximos de zero, é difícil prever e principalmente controlar, como e por quem os dados pessoais serão utilizados depois de compartilhados.

Além disso, a decisão de manter protegido um dado pessoal ou disponibilizá-lo varia conforme o contexto, o que, junto com a insegurança sobre os critérios de processamento e compartilhamento das informações, agrega um alto índice de incerteza sobre os riscos envolvidos na disponibilização.

**b. Benefícios de curto prazo e riscos de longo prazo**

As decisões sobre divulgação ou guarda de uma determinada informação (*trade-offs*) são, na maioria das vezes, intertemporais. Os benefícios aferidos com a divulgação, em regra, são imediatos, podendo ser intangíveis, como ao divulgar fotos para amigos em uma rede social, ou tangíveis, como a oferta de descontos, quando ocorrer uma transação direta. Já os custos são incertos e, geralmente, distantes no tempo, resultantes de um processo cumulativo de transações realizadas pelo indivíduo nos serviços oferecidos diretamente pelo fornecedor ou por meio de sua rede de capilaridade, principalmente lógica.

Um exemplo bastante claro da latência entre compartilhamento de dados e suas consequências pode ser visualizado nas campanhas de *behavioral targeting* ou simplesmente *retargeting*, muito comuns quando o usuário visita a página de um produto em um site de e-commerce específico e essa oferta o “persegue” nos banners e espaços publicitários de redes sociais e de sites que apresentam publicidade utilizando um serviço de gerenciamento e disponibilização de displays, como o Google AdSense, por exemplo.

**c. Trade-offs de privacidade misturam fatores tangíveis, intangíveis e incensuráveis**

As consequências de compartilhamento de dados envolvem riscos de três naturezas: tangíveis, como descontos de um player de e-commerce, diminuição



do potencial de contratação em virtude de verificação de comportamento em redes sociais, predição de preços de reserva que possibilita uma melhor individualização de preço; intangíveis, como o abalo psicológico decorrente de uma informação constrangedora ou cujo segredo o titular gostaria de manter, por motivos íntimos; e incomensuráveis, como os efeitos de uma sociedade de vigilância.

#### **d. A privacidade tem elementos de bens de consumo e de bens intermediários**

Segundo Goldfarb e Tucker (2019), a literatura econômica sobre privacidade, tanto offline quanto online, discute se a privacidade deve ser tratada como um bem de consumo, ou seja, aquele com valor em si mesmo, ou bens intermediários, cujo valor reside no modo como este bem modera a conquista de outro, ou seja, um bem de valor instrumental.

A literatura econômica sobre privacidade discute a questão de como a privacidade deve ser tratada em termos da função de utilidade dos consumidores. Os economistas devem tratar a privacidade como um bem intermediário - ou seja, um bem cujo valor simplesmente reside no modo como pode moderar a conquista de outro bem - ou como um bem final - ou seja, um bem que deve ser apreciado e valorizado por si próprio. Farrell (2012), em um trabalho dedicado ao tema, sugere uma terceira classe, na qual a privacidade se enquadraria: um bem intermediário onde o link com o produto de consumo não é absolutamente claro. A explicação de Acquisti, Taylor e Wagman (2016) ajuda a explicar a importância dessa controvérsia.

Atitudes em relação à privacidade capturam principalmente preferências subjetivas, isto é, as avaliações das pessoas sobre privacidade como um bem em si (privacidade como um bem de consumo). Mas essas avaliações são separadas das compensações reais que surgem após a retenção ou compartilhamento dos dados pessoais (da discriminação de preços ao roubo de identidade; dos cupons aos serviços personalizados), ou seja, do valor da privacidade como um bem intermediário (por exemplo, independentemente de uma pessoa pensar que "minha vida é um livro aberto, não tenho nada a esconder", ela continuará sofrendo danos tangíveis se for vítima de roubo de identidade)<sup>6</sup>.

#### **e. Nem sempre é claro como valorar a privacidade e os dados pessoais**

Não é fácil estabelecer os parâmetros ideais para se mensurar o valor dos dados pessoais. O ponto de referência deveria ser o preço que se recebe para divulgá-los ou o preço que deveria ser pago para protegê-los? Nas abordagens econô-

<sup>6</sup> No original: "Attitudes towards privacy mainly capture subjective preferences; that is, people's valuations of privacy as a good in itself (privacy as a final good). But those valuations are separate from the actual trade-offs that arise following the protection or sharing of personal data (from price discrimination to identity theft; from coupons to personalized services)—that is, from the value of privacy as an intermediate good (for instance, regardless of whether an individual thinks "my life is an open book, I have nothing to hide," that individual will still suffer tangible harm if she is a victim of identity theft)." (tradução deste mestrando)

micas tradicionais, o mercado captura o preço, refletindo os preços de reserva de diferentes compradores (acumuladores de dados) e vendedores (titulares de dados). Mas não existe, ainda, um mercado reconhecido de dados pessoais em que os titulares participam diretamente. Dados pessoais são comprados e vendidos, mas os titulares não têm acesso diretamente ao mercado, ou seja, eles não podem, de modo eficiente, colocar seus dados a venda. (ACQUISTI; TAYLOR; WAGMAN, 2016)

Tendo em conta as características inerentes das transações econômicas envolvendo dados pessoais, é importante voltar os olhos sobre os aspectos econômicos das transações, envolvendo dados pessoais, realizadas pelos serviços digitais disponibilizados sem contrapartida financeira pelos usuários. Praticamente toda a receita destas plataformas é gerada por publicidade, com a utilização de mecanismos de *two-sided matching*, descritos em maiores detalhes na Seção 3.1.2.

A primeira pergunta a ser respondida, para se entender a dinâmica das plataformas digitais financiadas por publicidade é identificar qual o seu diferencial, frente à publicidade entregue em outras mídias. Segundo Goldfarb (GOLDFARB, 2014), a principal diferença econômica da publicidade online fixa-se na substancial redução nos custos de segmentação (*targeting*). A segmentação possibilita uma aproximação mais precisa entre a oferta estabelecida pelo anunciante e os consumidores com maior propensão para adquirir a oferta anunciada. Como bem destaca Varian e Shapiro (1999), falando genericamente sobre tecnologia da informação, “no caso mais extremo, a tecnologia da informação possibilita um “mercado de um”, no sentido de que produtos altamente personalizados podem ser vendidos ao mais alto preço personalizado. Esse fenômeno é também conhecido como “customização em massa ou “personalização”.”<sup>7</sup>.

Neste ponto, a lógica econômica do modelo de publicidade online ganha contornos mais claros. Como as plataformas baseiam seus negócios na venda, aos anunciantes, da atenção escassa de consumidores (GOLDFARB; TUCKER, 2019), ou como designado neste trabalho, na venda do tempo dos seus usuários, disponibilizar mecanismos de segmentação significa, na prática, entregar para o anunciante o produto mais personalizado possível, ou seja, o usuário com maior potencial de realizar uma compra ao receber o impacto da ação publicitária. Como enfatizam Shapiro e Varian (1999), máxima personalização significa a possibilidade de maximização do preço. Isso explica, em grande medida a utilização dos leilões como modelo de venda, tendo em vista que este é um mecanismo clássico de maximização de preço, extremamente eficiente quando se tem um grande volume de compradores para um mesmo produto. Como a atenção de um potencial comprador altamente segmentado é um “produto”

<sup>7</sup> No original: “In the most extreme case, information technology allows for a “market of one”, in the sense that highly personalized products can be sold at a highly personalized price. This phenomenon is also known as “mass customization” or “personalization”.”

bem mais raro do que o público em geral e várias empresas de diferentes mercados têm interesse em segmentações de usuários similares, abre-se um espaço consistente de competição entre anunciantes o que reforça a opção pelo leilão como estratégia de maximização de preço.

Andando para o próximo elo da cadeia, a capacidade de segmentação de preço também se mantém na relação entre anunciante e usuário (consumidor). Neste ponto, há a possibilidade de segmentação de preço por parte do anunciante, a partir de um segundo grau de segmentação, onde diferentes produtos (ou versões do produto) são oferecidos a diferentes perfis de consumidores. Como o anunciante consegue selecionar uma mensagem mais específica para um perfil de usuário, também é possível oferecer a versão (*versioning*) mais adequada (aquela que maximiza o lucro) para aquele perfil específico. Esta estratégia de segmentação de preço é impulsionada, ainda, por outra característica que diferencia a publicidade em meio digital da publicidade em outros meios, a rastreabilidade, que será abordada mais à frente. Ainda em termos de segmentação, na relação entre anunciante e usuário, é possível a adoção de uma estratégia de terceiro grau, onde um mesmo produto é oferecido para públicos diferentes com preços diferentes. É o caso do *geo-pricing*, onde a determinação de preço se dá a partir da informação da localização do usuário no momento de realização da compra, como ocorreu no caso Decolar, onde os preços podiam variar, dependendo da localidade, em até 30% (MARCHETTI, 2018).

Cria-se, portanto, uma circunstância onde tanto a plataforma quanto o anunciante podem adotar comportamento de um quase monopolista, como destacam Shapiro e Varian (2004)

Mesmo em um ambiente competitivo, um vendedor pode ter um monopólio parcial na prestação de serviços personalizados, pois pode personalizar esses serviços à luz do comportamento de compra observado anteriormente. O equilíbrio resultante exibe uma forma de aprisionamento: alguns dos consumidores são leais aos fornecedores patrocinados originalmente, uma vez que esses fornecedores são capazes de fornecer serviços aprimorados personalizados que consideram particularmente valiosos<sup>8</sup>.

Como a capacidade de segmentação é o principal diferencial das plataformas online financiadas por publicidade, faz parte do modelo de negócios criar mecanismos que permitam melhorar cada vez mais seu potencial de segmentação. Esta é a principal razão econômica para a expansão das estratégias de capilaridade, tanto lógica quanto física, na busca por dados capazes de tornar mais eficiente este processo e individualizar de forma mais precisa os usuários, de modo a entregar um produto, para

<sup>8</sup> No original: "Even in a competitive environment, a seller may have a partial monopoly in providing personalized services since it can customize those services in light of previously observed purchase behavior. The resulting equilibrium exhibits a form of lock-in: some of the consumers are loyal to the vendors they originally patronized, since those vendors are able to provide personalized enhanced services that they find particularly valuable." (tradução deste mestrando)

os anunciantes, mais segmentado e, portanto, com maior possibilidade de aumento do preço, por segmentação. Além disso, toda a alocação dos espaços publicitários, incluindo as operações de leilão, são realizadas em tempo real, juntamente com a entrega do conteúdo principal ao usuário, o que exige imensa capacidade computacional. Estes dois aspectos, capilaridade (lógica e física) e poder computacional foram descritos no Capítulo 2.

A rastreabilidade, portanto, como já destacado anteriormente, é o segundo grande diferencial das plataformas financiadas por publicidade no meio digital. Não apenas porque as plataformas podem “fechar” de modo muito eficiente o público alvo, o que é absolutamente relevante, mas também porque o próprio anunciante tem mecanismos para fazer o *ajuste fino* (“*fine tuning*”) de suas campanhas de marketing. O marketing também é favorecido pelo efeito “fast-fail” (*erre rápido*) muito utilizado por *startups*, já que os baixos custos de segmentação e rastreabilidade possibilitam a execução de testes e avaliações sobre a eficiência das campanhas, realizadas em tempos muito curtos, antes do início das campanhas e, inclusive, durante todo o seu ciclo de vida, o que possibilita a melhor alocação do investimento de marketing, sempre contrastado com o resultado final, em número de conversões.

O entendimento claro dos mecanismos de segmentação e, conseqüentemente, de rastreabilidade (*tracking*), bem como das dificuldades de tomada de decisão relativas à retenção ou compartilhamento de dados pelos indivíduos, possuem importância fundamental para o entendimento do papel da regulação, pois, como bem destacam Goldberg e Tucker (2019), a regulação da privacidade impõe custos na rastreabilidade dos fluxos de informação e o efeito desses custos no bem estar podem ser ambíguos, tendo em vista que, de um lado, o consumidor pode ter acesso a produtos mais alinhados com suas expectativas, o que tende a aumentar o seu bem estar, mas de outro cria mecanismos de segmentação que permitem inferir o preço de reserva do consumidor e, com isso, potencialmente, diminuir o excedente do consumidor com estratégias eficientes de segmentação de preço.

Atualmente, o principal mecanismo regulatório utilizado nestes casos é a busca, por parte da plataforma e dos anunciantes (neste caso para utilização de mecanismos de rastreamento), do consentimento dos indivíduos para o tratamento dos dados pessoais. O consentimento, portanto, cria um custo para o compartilhamento, inclusive com implicações concorrenciais (GOLDFARB; TUCKER, 2019). Além disso, todas as peculiaridades das transações envolvendo dados pessoais, que tornam complexas as tomadas de decisão sobre este tema, são sentidas pelos indivíduos, no caso do consentimento, na maioria das vezes, no momento de ingressar em determinada plataforma, sem que ele tenha acesso a um conjunto adequado de informações. Como bem destaca Acquisti, Taylor e Wagman (2016), compilando pensamentos de vários autores:

existem preocupações sobre o fato de que as tecnologias de rastreamento geralmente são invisíveis para os usuários finais (Smith 1999), por isso existe uma significativa falta de conhecimento e entendimento entre os consumidores em relação à extensão, natureza e profundidade das técnicas de segmentação (McDonald e Cranor 2010). Mesmo consumidores sofisticados podem não ser capazes de evitar serem rastreados, pois o setor de publicidade e dados frequentemente encontra novas maneiras de rastrear e identificar usuários depois que os consumidores aprendem e adotam medidas para combater as formas de rastreamento existentes (Hoofnagle et al. 2012).<sup>9</sup>

A abordagem da economia da privacidade, portanto, tem o grande mérito de explicitar o caráter transacional do fluxo de dados, o que é especialmente valioso quando se aborda aplicações que baseiam seus modelos de negócio em segmentação e rastreamento. Neste caso, no nível mínimo de proteção dos dados pessoais como parte integrante da personalidade, o fluxo de dados (sua existência ou seu volume) deve ser fruto de um contrato entre as partes, com participação garantida ao indivíduo, afastando-se por completo a possibilidade de uma decisão unilateral da plataforma.

Neste sentido, mirando as legislações de proteção de dados pessoais como a GDPR e a LGPD, em transações envolvendo este tipo de finalidade, não há espaço para a realização de tratamento de dados pessoais baseando-se em critérios unilaterais como, por exemplo, o legítimo interesse da própria plataforma ou de terceiros. Mesmo o consentimento, base legal consagrada como a principal viabilizadora do tratamento de dados pessoais por estas plataformas, precisa ser visto como um contrato efetivo, dando maior controle, aos indivíduos, quanto ao uso de seus dados, impactando de modo mais contundente não apenas na realização das ações de tratamento, mas sobre os resultados gerados por estas operações de tratamento, tema que será abordado no próximo capítulo.

### 3.1.2 Plataformas, mercados de dois lados e monopólio

Serviços digitais oferecidos sem a necessidade de um pagamento direto dos usuários operam, essencialmente, em mercados bilaterais (de dois lados ou *two-sided markets*). Outros serviços, não necessariamente gratuitos, como aplicações de transporte individual e caronas, aplicações de compartilhamento de imóveis ou de entrega de comida, também operam em mercados desta categoria.

Mercados bilaterais são aqueles que apresentam um tipo específico de efeito de rede<sup>10</sup>.

<sup>9</sup> No original: "concerns exist over the fact that tracking technologies are often made invisible to end-users (Smith 1999), whereby a significant lack of awareness and misconception exists among consumers regarding the extent, nature, and depth of targeting techniques (McDonald and Cranor 2010). Even sophisticated consumers may not be able to avoid being tracked, as the advertising and data industry has often found new ways of tracking and identifying users after consumers had learned about and adopted measures to counter existing forms of tracking (Hoofnagle et al. 2012)." (tradução deste mestrando)

<sup>10</sup> Efeito de rede ou externalidade de rede, genericamente considerado, pode ser definido como um

Os mercados bilaterais não nasceram com as plataformas digitais, apenas se tornaram muito mais comuns, tendo em vista a forte redução nos custos de distribuição trazida pela Internet. Um bom exemplo fora do mundo das plataformas é o caso da Adobe, com o PDF, um formato de arquivo desenvolvido pela empresa. Quanto mais pessoas podem visualizar arquivos neste formato, mais pessoas se interessarão em produzi-los. Assim, quanto mais pessoas possuírem um softwares de leitura de PDFs, mais fácil ficará para a Adobe vender seus produtos e tecnologias de criação de PDFs, como o Adobe Acrobat Pro. Neste contexto, pode ser interessante para a empresa facilitar o acesso aos softwares de leitura, tornando-os gratuitos, como faz a Adobe com o seu Acrobat Reader (VARIAN, 2015).

Sistemas de busca são o exemplo clássico de mercados bilaterais em ambiente digital, sendo que as mesmas características são observadas em outros tipos de plataforma que oferecem serviços sem uma contrapartida financeira do usuário final. Utilizando o Google como exemplo e a explicação de Varian (2006), pode-se classificar o Google como um match-maker, literalmente “casamenteiro” ou, como preferiu Varian, “*yenta*”, a palavra Yiddish equivalente. Do lado da busca, a plataforma promove o encontro das pessoas com as informações que elas procuram. Do lado da publicidade, faz o encontro de pessoas que querem vender algo àquelas que querem comprá-las. Esta visão do segundo lado é bem alinhada ao discurso das plataformas. Visto de um outro ângulo, como já mencionado anteriormente, vendem a valiosa atenção de um usuário altamente segmentado, cujo acesso é concorrido.

Este é um negócio intensivo de escala. Varian apresenta números de 2006: “uma boa taxa de *clickthrough* [conversão de cliques] seria 3% e uma típica taxa de conversão (compra) em torno de 3%. Isso significa que menos de um em cada mil pessoas que veem um anúncio compra o produto anunciado.”<sup>11</sup>. A empresa de otimização de publicidade digital WordStream (2019) fez um levantamento das taxas de clique e retorno de seus clientes na rede, em 2019, e os valores obtidos foram, respectivamente, 3,17% e 3,75%, números muito próximos dos apresentados por Varian, há mais de 13 anos, principalmente ao considerar que, pelo menos em tese, esses números são de campanhas já otimizadas.

A força da rastreabilidade como diferencial competitivo frente às mídias tradicionais, como exposto na Seção 3.1.1, fica evidente com esses números. Se o anunciante

---

tipo de externalidade onde a utilidade de um bem para uma pessoa depende do número de outras pessoas que consomem um outro bem, seja da mesma categoria ou de outra. Já as externalidades, do ponto de vista econômico, podem ser classificadas como de consumo ou na produção. Uma externalidade de consumo ocorre quando um consumidor se preocupa diretamente com a produção ou o consumo de outro agente. Já a externalidade na produção aparece quando as possibilidades de produção são influenciadas pelas escolhas de outra empresa ou de outro consumidor (VARIAN, 2015)

<sup>11</sup> No original: “A good ad clickthrough rate might be 3% and a typical conversion (purchase) rate might also be around 3%. This implies that fewer than one out of a thousand people who see the ad actually buy the product being advertised.”

consegue rastrear o número total de conversões (dado necessário para se chegar à taxa de conversão) e, também, o volume total investido, chega-se facilmente ao custo médio de conversão. Com todos esses dados acessíveis, a área de marketing do anunciante e suas agências conseguem medir a eficiência de campanhas de modo muito mais preciso do que em mídias tradicionais, onde os mecanismos de rastreabilidade das ações dos consumidores não são eficientes.

Efeitos ou externalidades de rede, que são efeitos de escala do lado da demanda, são classificados em duas categorias. O efeito de rede direto, ou simplesmente efeito de rede, acontece quando a demanda pelo bem depende da quantidade de pessoas que o compraram. Este efeito pode ou não aparecer em um mercado bilateral. O exemplo principal, no mundo digital, são as redes sociais, onde o aumento do número de pessoas conectadas à rede a torna mais atraente para novos usuários. Obviamente, esse efeito começa a ser percebido a partir de uma massa crítica de usuários ou compradores. Uma quantidade que não é pequena e que muitas vezes pode exigir investimentos massivos para aquisição de base usuários. Esse efeito começou a ser observado intensamente, como descreve Varian (2019), a partir da análise de redes de telefonia, sendo primeiramente descrito por Jeffrey Rohlfs, pesquisador do Bell Labs.

Já o efeito de rede indireto está sempre presente em um mercado de dois lados. No efeito de rede indireto, a demanda por um determinado produto ou serviço depende da quantidade de pessoas que compram ou utilizam um outro produto ou serviço. É exatamente o que acontece com os sistemas de busca e as redes sociais. Quanto mais pessoas utilizam uma determinada plataforma, mais anunciantes se interessarão em anunciar na plataforma, ou seja, há um aumento da demanda por anúncios com o aumento do número de pessoas que utilizam a plataforma.

Um outro aspecto relevante das plataformas digitais oferecidas gratuitamente diz respeito à sua posição de intermediária e o impedimento de um contato direto entre os grupos de clientes (usuários e anunciantes) sem sua participação direta. A definição de Evens e Schmalensee (2013) de plataforma bilateral (multilateral ou catalisador como os autores também as designam) deixa claro seu modo de funcionamento sob esta perspectiva. Para eles, uma plataforma de dois lados

possui (a) dois ou mais grupos de clientes; (b) que precisam um do outro de alguma maneira; (c) mas que não podem capturar o valor de sua atração mútua por conta própria; e (d) confiam no catalisador para facilitar a criação de valor nas interações entre eles<sup>12</sup>

Essa característica de segregação entre os dois grupos tem uma importância singular na avaliação da privacidade. Primeiro porque, para existir a separação, os

<sup>12</sup> No original: "has (a) two or more groups of customers; (b) who need each other in some way; (c) but who cannot capture the value from their mutual attraction on their own; and (d) rely on the catalyst to facilitate valuecreating interactions between them." (tradução deste mestrando).

dados pessoais dos usuários nunca são passados para os anunciantes. Por isso, um dos grandes argumentos das plataformas como justificativa de suas atividades reside no fato de que não há venda direta de dados pessoais. Por outro lado, suas operações tornam-se verdadeiras concentradoras de dados pessoais que, junto com as estratégias de capilaridade lógica e física para aumentar a capacidade de captação, transformam essas plataformas em imensas estruturas de segmentação e perfilização de pessoas, decidido não apenas quem será o vencedor de cada leilão de anúncio, mas também o conteúdo visto e as interações realizadas pelos usuários no uso normal da plataforma. Esse imenso poder de criação de perfis será intensificado com o aumento da adoção de soluções de inteligência artificial. Como bem coloca Cass Sunstein (2017):

Com o crescimento da inteligência artificial, os algoritmos melhorarão imensamente. Eles aprenderão muito sobre você, e eles saberão o que você quer ou vai gostar antes de você e melhor do que você. Eles vão mesmo conhecer suas emoções, novamente antes e melhor do que você, e eles serão capazes de imitar as emoções por conta própria.

(...)

O aprendizado da máquina [machine learning] pode ser usado (e provavelmente está sendo usado) para produzir distinções finas. É fácil imaginar uma grande quantidade de classificação, não apenas entre direita e esquerda no âmbito político, mas também com detalhes sobre os assuntos que mais lhe interessa e suas visões prováveis sobre essas questões (imigração, segurança nacional, igualdade, e meio ambiente). Para dizer o mínimo, estas informações poderão ser úteis para outras pessoas - gerentes de marketing, anunciantes, captadores de recursos e mentirosos, incluindo extremistas políticos<sup>13</sup>.

### 3.1.2.1 Efeitos de rede e competição

Uma questão fundamental que se coloca, ao avaliar o efeito de rede nas plataformas digitais, diz respeito às suas contribuições para o surgimento de monopólios. Como destacam Shapiro e Varian (1999), os efeitos de rede criam uma situação onde, atingida uma determinada massa crítica, o mercado é construído por si mesmo. Uma decorrência dessa expansão em cascata, naturalmente, é a concentração de mercado. Por esse motivo, mercados onde o efeito de rede está presente geralmente atraem a atenção dos reguladores da concorrência.

Em um relatório recente, sobre a necessidade de um novo framework de competição para a economia digital, a comissão denominada “Competition Law 4.0”, ligada

<sup>13</sup> No original: “With the rise of artificial intelligence, algorithms are bound to improve immeasurably. They will learn a great deal about you, and they will know what you want or will like, before you do, and better than you do. They will even know your emotions, again before and better than you do, and they will be able to mimic emotions on their own. (...) Machine learning can be used (and probably is being used) to produce fine-grained distinctions. It is easy to imagine a great deal of sorting—not just from the political right to the political left, but also with specifics about the issues that you care most about, and your likely views on those issues (immigration, national security, equality, and the environment). To say the least, this information can be useful to others— campaign managers, advertisers, fund-raisers and liars, including political extremists.” (tradução deste mestrando)



ao Ministério de Assuntos Econômicos e Energia da Alemanha, se posicionou da seguinte maneira sobre a relação entre efeitos de rede e concentração de mercado (COMMISSION 'COMPETITION LAW 4.0', 2019):

Efeitos de rede positivos levam a tendências de concentração nos mercados de plataforma (veja o Capítulo II acima). Eles podem levar ou fortalecer uma posição dominante já existente. Como um grande número de usuários e opções de matching tornam as plataformas atraentes, a concentração em uma ou poucas plataformas pode ser eficiente. No entanto, efeitos de rede positivos também podem levar a altas barreiras de entrada. Uma vez atingida uma posição dominante, ela pode se tornar rapidamente entrincheirada, tornando quase impossível para os concorrentes (potenciais) atacarem. Isso é chamado de "tipping", ou seja, quando um mercado inicialmente competitivo se torna um mercado monopolista ou altamente concentrado<sup>14</sup>.

Esta posição da Comissão alemã é relevante, principalmente se confrontadas com autores como Varian (2019) e Tucker (2018) que minimizam os efeitos de rede como fenômenos que favoreçam decisivamente o surgimento de monopólios ou uma concentração de mercado. Independente da relevância como fator originário, os efeitos de rede criam barreiras importantes à concorrência quando há uma situação de monopólio ou de grande concentração de mercado.

A existência de grande concentração de mercado também pode favorecer o aparecimento de efeitos colaterais, relativos à concorrência, decorrentes da regulação de privacidade, ao intensificar condições que favorecem a consolidação de monopólios. Acquiti, Taylor e Wagman (2016) esclarecem esta relação:

A distribuição ou proteção dos dados pessoais também pode influenciar a competição no mercado. Campbell, Goldfarb e Trucker (2015) demonstram que, se a regulamentação de privacidade depender apenas da imposição do consentimento (opt-in), a consequência não intencional poderá ser a consolidação de monopólios. Os autores mostram que os consumidores são mais propensos a conceder o seu consentimento para grandes grupos, com amplo escopo, ao invés de empresas menos consolidadas. Assim, se a regulação se concentra apenas na aplicação de uma abordagem baseada em opt-in, os usuários podem ser menos propensos a tentar serviços de empresas de menor porte e novas entrantes, criando potenciais barreiras de entrada e levando a um "monopólio natural" em que a economia de escala incluiria a proteção da privacidade<sup>15</sup>.

<sup>14</sup> No original: "Positive network effects lead to concentration tendencies on platform markets (see Chapter II above). They may lead to or strengthen an existing dominant position. Since a large number of users and matching options are often what make platforms attractive, concentrating on one or a few platforms can be efficient. However, positive network effects can also lead to high barriers to market entry. Once a dominant position has been attained, it can quickly become entrenched, making it almost impossible for (potential) competitors to attack. This is referred to as 'tipping', i.e. when an initially competitive market tips into a monopolistic or highly concentrated market." (tradução deste mestrando)

<sup>15</sup> Texto original: "The sharing or protection of consumer data can also influence market competition. Campbell, Goldfarb, and Tucker (2015) demonstrate that, if privacy regulation only relied on enforcing opt-in consent, an unintended consequence may be the entrenching of monopolies. The authors show that consumers are more likely to grant their opt-in consent to large networks with a broad scope, rather than to less established firms. Hence, if regulation focuses only on enforcing an opt-

Neste sentido, mesmo que os efeitos de rede não tenham relação direta com as causas da concentração de mercado, o fato de um produto ou serviço, sob a influência deles, apresentar uma curva acentuada de crescimento de adoção, já se configura como um motivo relevante para a avaliação dos impactos destes efeitos em circunstâncias que possam ser enquadradas como abuso de posição dominante.

### 3.1.2.2 *Data-driving network effects*

Em 2016, Maurice E. Stucke e Allen P. Grunes, lançaram o livro *Big Data and Competition Policy*, onde cunharam o termo '*Data-opólio*' ('*Data-opoly*'), onde expõem a necessidade de formuladores de políticas e reguladores da concorrência adotarem novos parâmetros capazes de identificar comportamentos e situações anti-competitivas nos novos mercados que envolvem o tratamento massivo de dados. Para os autores, os parâmetros adotados para avaliação da competição em indústrias tradicionais não são adequados, principalmente por não considerarem adequadamente os "efeitos de rede orientada a dados" ("*data-driven network effects*").

Para os autores, *efeitos de rede orientada a dados* podem ser divididos em quatro categorias: (a) efeitos de rede clássicos; (b) efeitos de rede decorrentes da escala de dados; (c) efeitos de rede do escopo de dados e (d) efeitos de rede de um lado de uma plataforma que podem se espalhar para o outro(s) lado(s). (STUCKE; GRUNES, 2017)

A expressão *data-driven network effects* tem se espalhado e hoje vários documentos e artigos a utilizam para nomear genericamente os efeitos característicos dos modelos de negócio com arquitetura de rede e grande acumulação e tratamento de dados. Não há, na formulação proposta por Stucke e Grunes um rigor quanto ao uso da expressão *efeito de rede*, do ponto de vista econômico, tendo em vista que apenas a primeira categoria se encaixa no conceito econômico de efeito de rede, como uma externalidade do lado da demanda. Isso não significa que os outros efeitos não existam, nem que são pouco relevantes ou gerem pouca influência do ponto de vista da concorrência, mas a união de todos sob uma expressão guarda-chuva pode dificultar a análise e o impacto de cada um deles.

Neste trabalho, além dos efeitos de rede clássicos, ou seja, externalidades do lado da demanda, já abordados no item anterior, serão tratados, neste item, o efeito de escala baseado em dados e, no próximo, os efeitos do custo zero, do lado usuário, um caso particular, aplicável às plataformas aqui estudadas, da quarta categoria indicada pelos autores.

O efeito de escala de dados (equivalente à categoria (b) apresentada por Stucke

---

in approach, users may be less likely to try out services from less established firms and entrants, potentially creating barriers to entry by leading to a "natural monopoly" in which scale economics include privacy protection. (tradução deste mestrando)."

e Grunes) é, como descreve Varian (2019), uma externalidade do lado da produção (*supply-side*) e não uma externalidade do lado do consumo (ou da demanda ou *demand-side*) como são os efeitos de rede. Esse efeito de escala de dados pode ser enquadrado como um fenômeno conhecido, na economia, como “*learning by doing*”, onde quanto maior o número de usuários, maior a quantidade de informações que a plataforma tem sobre eles e, a partir da análise de seus comportamentos, a plataforma aumenta sua eficácia na entrega de seus produtos a seus clientes. Neste caso específico, entrega resultados para os usuários mais afinados com suas preferências e, no caso dos anunciantes, fecha melhor o alvo para que as campanhas possam gerar mais resultados.

Neste ponto, é importante ter atenção ao escopo e à abrangência do *learning by doing*, principalmente quanto ao acervo de dados disponíveis para a plataforma. Não é possível restringir o entendimento deste efeito apenas às interações produzidas no âmbito de uma única aplicação em situações onde as plataformas possuem mais de um produto ou tenham uma ampla capilaridade, tanto lógica como física, capaz de captar dados pessoais mesmo em momentos em que o indivíduo não está utilizando diretamente a solução. O risco de se negligenciar este escopo mais abrangente de origens de dados é grande e um exemplo pode ajudar a evidenciar este risco.

Em 2008, Google e Yahoo! anunciaram uma *joint venture*, onde o Google passaria a entregar anúncios nos websites do Yahoo! que, em contrapartida, receberia uma parte da receita gerada. Em 5 de novembro de 2009, o acordo foi abandonado, depois da sinalização de oposição ao acordo pela Divisão Antitrustes, do Departamento de Justiça dos Estados Unidos da América (EUA). Ao descreverem o caso, depois de participarem do processo de investigação realizado pela Divisão Antitruste, Heyer Shapiro e Wilder (2009) fazem uma boa descrição do “*learning by doing*”.

porque a escala é tão importante nos negócios de publicidade em buscas, o efeito do Yahoo! terceirizar negócios significativos para o Google poderia precipitar uma espiral descendente, com sérias consequências para a competitividade futura do Yahoo!. As plataformas de publicidade de busca são bem-sucedidas, em grande parte, na medida em que promovem encontros entre usuários e anúncios relevantes e o *learning by doing* é uma grande parte do que faz essas plataformas melhorarem. Saber quais anúncios provavelmente geram o interesse de um usuário é, em parte, um jogo de números: quanto mais oportunidades a plataforma tiver para observar usuários semelhantes respondendo a anúncios semelhantes, melhor será a capacidade da plataforma de corresponder anúncios a qualquer usuário individual<sup>16</sup>.

<sup>16</sup> No original: “because scale is so important in the search advertising business, the effect of having Yahoo! outsource significant business to Google could precipitate a downward spiral, with serious consequences to Yahoo!’s future competitiveness. Search advertising platforms are successful largely to the extent that they match users with relevant ads, and “*learning by doing*” is a big part of what helps these platforms improve. Knowing which ads are likely to generate a user’s interest is in part a numbers game: The more opportunities that the platform has to observe similar users responding to similar ads, the better is the platform’s ability to match ads to any individual user. The greater the increased profits to Yahoo! from outsourcing, the more outsourcing Yahoo! would have found profitable.” (tradução deste mestrando)

Para os reguladores, portanto, neste caso específico o *learning by doing* refere-se especificamente à análise dos dados resultantes dos próprios processos de entrega de publicidade, ou seja, o acumulado de resultados dos leilões passados ajuda a aumentar a acurácia dos próximos leilões. Esse efeito é importante, mas não representa a totalidade dos dados utilizados para realizar a segmentação. Outros critérios são utilizados, a partir da análise de dados coletados fora do processo de leilão, que classificam o indivíduo alvo a partir do conjunto de informações que a plataforma concentra sobre o usuário. Essas informações maximizam a acurácia e influenciam nos leilões, neste caso específico.

Por isso, a análise do “*learning by doing*” deve ser realizada, para fins de avaliação de comportamento anti-competitivo, considerando o acervo total de dados a disposição da plataforma, o que exige uma análise bem mais ampla, não apenas focada no serviço entregue ao usuário final, mas que leve em consideração toda cadeia, na maioria das vezes de altíssima complexidade, de captação de dados que pode influenciar no resultado final. Essa visão mais ampliada ajuda a tornar mais claro os comportamentos de vigilância dos *players* que atuam em mercados altamente concentradores de dados pessoais e, conseqüentemente, possibilita uma atuação mais contundente não apenas nas análises de fusões e aquisições, mas principalmente na identificação de comportamentos de abuso de posição dominante, onde o fornecedor consegue diminuir, de modo significativo, o excedente do consumidor ou gerar riscos relevantes aos consumidores pela existência de vieses na apresentação dos resultados.

### 3.1.2.3 Preço zero do lado do usuário

O que significa, para o consumidor, o preço grátis? Para Dan Ariely, zero não é só um preço. “Zero é um botão emocional - uma fonte de empolgação irracional”.

Para demonstrar o impacto psicológico do preço zero, Dan Ariely e Kristina Shampiner, então aluna de doutorado no MIT, fizeram um experimento. Posicionaram, em um grande prédio público, uma mesa com chocolates de duas marcas: trufas Lindt e Kisses, da marca Hershey. Há uma grande diferença de qualidade entre os dois produtos. Enquanto o chocolate Lindt é fabricado na Suíça, com os melhores cremes de cacau e tinha um preço, na época, de US\$ 0,50 por unidade, em compras em grande escala, os chocolates da Hershey são fabricados na Pensilvânia, em uma cidade de mesmo nome e eram produzidos, na época, a uma escala de 80 milhões por dia. Na mesa, havia um aviso que dizia “Um chocolate por cliente”. Em um primeiro momento, os pesquisadores definiram os preços em US\$ 0,15 para a unidade de Lindt e US\$ 0,01 para a unidade do chocolate da Hershey. Como resultado, 73% dos consumidores escolheram o chocolate suíço, contra 27% da marca americana. Em outro momento, os pesquisadores fizeram um decréscimo de 1 centavo no preço de cada chocolate,

assim, o Hershey passou a ter preço zero e o Lindt passou a custar US\$ 0,14. O resultado: 69% dos consumidores optaram pelo chocolate da Hershey (no primeiro experimento foram 27%) e apenas 31% escolheram comprar o Lindt (ARIELY, 2008).

A força do preço zero é tão grande que as pessoas até pagam por mês para poder aproveitá-lo. O caso da Amazon Prime é emblemático. E o título do *press release* de lançamento do produto no Brasil dá a dimensão desse poder (grifo nosso): "Amazon Prime chega ao Brasil em seu maior lançamento já feito em um país — *frete grátis e rápido, acesso a entretenimento e promoções exclusivas, por apenas R\$9,90 ao mês*" (AMAZON, 2019).

O próprio Ariely sugere uma explicação para a sedução do preço zero: "a maioria das transações tem um aspecto positivo e um negativo, mas quando algo é grátis, esquecemos o negativo. (...) temos um medo intrínseco da perda. O verdadeiro chamariz do grátis está vinculado a esse medo. Não existe possibilidade visível de perda quando escolhemos alguma coisa grátis (não é preciso pagar)" (ARIELY, 2008).

Um olhar com este enfoque é necessário ao avaliar as plataformas digitais utilizadas sem contrapartida financeira pelos usuários. Esse é exatamente o caso. Algo vendido como se fosse grátis e que, por isso, atrai todos os efeitos emocionais que favorecem o consumo, pela ausência de um parâmetro de contrapartida ou, nas palavras de Ariely, sem que fique clara a parte negativa da transação. Acresça-se a isso todas as dificuldades na tomada de decisão sobre dados pessoais, que decorrem das características peculiares destas transações, tais como os benefícios de curto prazo e os riscos de longo prazo, os riscos intangíveis ou incomensuráveis frente ao benefício tangível de se utilizar um serviço a preço zero e a imensa dificuldade de se valorar os dados pessoais. Tudo isso contribui para a construção de um cenário de *oferta perfeita* e com fatores negativos muito pouco perceptíveis para o usuário não *expert*.

Neste ponto, é importante notar uma peculiaridade relacionada ao termo *consentimento*, utilizado pelas legislações de proteção de dados, como a GDPR e a LGPD, para dar contorno à hipótese legal que, em grande medida, suporta os tratamentos de dados pessoais, para fins específicos do controlador, em situações como a disponibilização de espaços publicitários em plataforma utilizadas sem contrapartida financeira do usuário. A ideia de consentimento, ou seja, de dar permissão, anuência, aquiescência (DICIONÁRIO MICHAELIS, 2020), suprime muito da carga transacional, dando a sensação para o usuário que esta é uma autorização para uso gratuito dos dados pessoais e não uma das contraprestações (o tempo de uso que cria as oportunidades de veiculação é outra contraprestação) efetivamente pagas, pelo usuário, para utilização dos serviços. A separação, portanto, entre consentimento e gratuidade, reforça a ideia de ausência da parte negativa da transação e contribui com o alto poder de persuasão das plataformas para atrair novos usuários que poderão utilizá-las "a custo zero".

No mesmo *paper* em que apresentam os resultados da experiência com os chocolates, os autores citam um outro caso, desta vez real. Quando a Amazon introduziu o frete grátis, a partir de um determinado valor de venda, em diversos países da Europa, utilizou uma estratégia diferente na França. Lá, ao invés de tornar o frete gratuito, posicionou o preço em um franco (algo em torno de dez centavos de dólar), à época. Os resultados de aumento de venda foram muito mais expressivos nos países que adotaram o frete grátis comparado ao observado na França, onde optou-se por um preço negligenciável. Os autores, então, fazem uma constatação interessante (SHAMPANIER; MAZAR; ARIELY, 2007): "Este exemplo também sugere que, ao tentar usar a agregação (*bundling*) de um bem barato para aumentar as vendas de outro bem, pode ser sensato reduzir o preço do bem barato e oferecê-lo gratuitamente.<sup>17</sup>"

O *bundling* também é uma ferramenta bastante utilizada pelas plataformas, como meio de atrair e manter conectados os usuários. Como exemplos, tem-se o imenso rol de produtos Google, cujo uso é facilitado toda vez que mantemos nossos *browsers* continuamente conectados utilizando-se a conta Google, ou a integração cada vez mais intensa entre as plataformas de rede social do Facebook. Mas neste ponto outra característica chama a atenção. Como abordado no primeiro capítulo, praticamente todo conteúdo apresentado por estas plataformas é utilizado, por elas, de forma gratuita e os dados pessoais também são utilizados sem uma contrapartida efetiva. O resultado prático disso é um custo marginal próximo de zero. Como o custo marginal é próximo de zero, é possível escolher de quais ou de qual lado, e sobre quais transações, ficará posicionado o preço. Neste sentido, posicionar o preço totalmente do lado do anunciante, além de favorecer o efeito de rede, pela eliminação de barreiras para o ingresso de usuário, também aproveita toda a carga psicológica positiva associada ao preço zero.

Um outro aspecto bastante relevante do preço zero para o usuário final, se refere ao fato de que, ao levar a zero o preço ao usuário final, as plataformas estabelecem um modelo de negócio baseado em pagamento por terceiros (*third-party payment business model*), que pode reforçar os efeitos monopolistas. Neste sentido, Clemons e Madhani (2010) resumem, tendo como referências o Google e seu sistema de busca:

1. O preço do Google é dissociado da disciplina de mercado porque o usuário e o pagador não são a mesma pessoa, portanto, os preços elevados cobrados não alteram o comportamento do usuário. Assim, os monopólios baseados em pagamento por terceiros podem ser estáveis. Mais uma vez, no caso específico do Google, mesmo que o Google fosse considerado um monopolista caro, ninguém está em posição de oferecer pesquisas que os consumidores acreditam serem mais baratas. Isso ocorre porque a busca não pode ser mais barata para os consumidores: os consumidores pensam que já é mais barato do que grátis porque não lhes custa nada e a eles são fornecidos uma ampla

<sup>17</sup> No original: "This example also suggests that when trying to use bundling with a cheap good in order to bring up the sales of another good, it might be wise to go all the way down with the cheap good and offer it for free." (tradução deste mestrando)

gama de serviços auxiliares gratuitos. 2. Se a busca for considerada uma facilidade essencial e se o Google for o sistema de busca escolhido por uma maioria estável de consumidores, então este é o mecanismo de busca onde as empresas devem aparecer. Os concorrentes continuarão a oferecer, e se houver danos, então o dano continuará a ocorrer. 3. Além disso, porque os leilões de palavras-chave e a pesquisa patrocinada fornecem ao Google o fluxo de receita que atualmente desfruta, então a capacidade de direcionar os consumidores e a capacidade de sufocar a concorrência em uma variedade de mercados que o Google subsidia permanecerá<sup>18</sup>

Mais uma vez, o *bundling* (a agregação de vários produtos disponibilizados aos usuários) aparece como mecanismo de reforço de gratuidade, tendo em vista que, em geral, as plataformas nunca cobram, em dinheiro, do usuário final. Além disso, o modelo de negócio baseado em pagamentos de terceiros permite um descolamento entre a curva de crescimento de usuários e a curva de crescimento de faturamento, o que pode criar um efeito de rede em termos de faturamento, ou seja, uma curva de crescimento de faturamento que acelera (cresce mais rapidamente) com o incremento do número de usuários. O próximo item apresenta uma prova, com dados reais, de que este aumento da velocidade de crescimento do faturamento realmente existe.

É importante sempre ter em mente que, apesar do preço ser zero, em termos monetários, a remuneração pelo uso, por parte dos usuários, não é indireta, tendo em vista que a cessão dos dados pessoais, na relação com as plataformas digitais, configura-se como uma contraprestação efetiva, uma remuneração direta, não pecuniária, realizada pelo usuário para ter acesso aos serviços. Essa relação será mais profundamente detalhada na Seção 4.2.2.1

#### 3.1.2.4 Lei de Metcalfe e o efeito de rede

Bob Metcalfe marcou seu nome na história da computação quando, em 22 de maio de 1973 circulou um memorando no Xerox Palo Alto Research Center (PARC) mostrando como uma rede local (*Local Area Network* ou, simplesmente, LAN) deveria funcionar. Assim nasceu o protocolo Ethernet.

Em 1979 foi um dos cofundadores da 3Com, uma empresa de tecnologia, dedicada ao desenvolvimento de equipamentos e soluções de rede, que chegou a faturar

<sup>18</sup> No original: "1. Google's pricing is decoupled from market discipline because the user and the payer are not the same; hence, high prices charged do not alter user behavior. Thus, third-party payer monopolies may be stable. Again, in the specific instance of Google, even if Google were found to be an expensive monopolist, no one is in a position to offer search that consumers believe is cheaper. This is because search could not be cheaper for consumers: consumers think it is already cheaper than free because it costs them nothing, and they are provided with a wide range of free ancillary services. 2. If search is found to be an essential facility and if use of Google is the stable search engine decision of most consumers, then this is the search engine on which corporations have to appear. Bidders will continue to bid, and if there is harm, then harm will continue to occur. 3. Moreover, because key word auctions and sponsored search provide Google with the revenue stream it currently enjoys, then the ability to misdirect consumers and the ability to stifle competition in a range of markets that Google subsidizes will remain" (tradução deste mestrando)

US\$ 5,7 bilhões, em 1999, quando foi vendida para a Hewlett-Packard (HP). Mas, no começo, vender placas de rede para os recém lançados computadores pessoais (PC)s da IBM, não era tarefa fácil. Principalmente porque, naquela época, cada placa custava próximo de US\$ 1.000 e exigia um esforço extra de cabeamento para conectar os computadores. O grande argumento de vendas era a possibilidade de compartilhamento de impressoras e unidades de disco. A impressora Laser Writer, da Apple, lançada em 1985 custava US\$ 7.000. Mas mesmo com a possibilidade de compartilhar recursos valiosos, os clientes tinham a sensação de que uma rede com uma pequena quantidade de computadores conectados não tinha muita utilidade. Então, em uma apresentação para a força de vendas da 3Com, Metcalfe projetou, em um slide de 35mm, a figura de um gráfico que representava a relação entre o valor de uma rede (V) e a sua quantidade de nós (N), ou dispositivos conectados: com N nós, cada um se conecta a (N - 1) outros nós e V deveria ser proporcional ao número de possíveis conexões entre os nós, ou seja,  $N \times (N - 1)$  ou, aproximadamente,  $N^2$ .

$$V \sim N^2 \quad (2)$$

Estava formulada o que depois ficou conhecida como Lei de Metcalfe, que descreve a evolução de um efeito de rede. E os efeitos desta formulação (função de ordem quadrática ou de crescimento quadrático) são fáceis de serem observados. Por exemplo, ao considerarmos uma rede com 10 nós, tem-se um valor da rede de 100. Já uma rede de 1.000 nós gera um valor de 1.000.000.

Passados quarenta anos da criação do protocolo Ethernet e trinta anos da primeira formulação da Lei, Metcalfe revisitou a sua lei e escreveu um artigo, para o periódico *Computer*, publicado pela Institute of Electrical and Electronics Engineers (IEEE). Todo relato feito acima foi extraído deste artigo (METCALFE, 2013).

Até aquele momento, a Lei de Metcalfe não tinha sido provada empiricamente. Como o próprio autor diz, essa não foi a primeira lei desta natureza. David Sarnoff, que liderou a RCA dos anos 1930 a 1970, definiu o valor de uma rede na transmissão *broadcast* de TV como sendo proporcional ao número de expectadores:  $V \sim N$ . Algumas variações da Lei de Metcalfe também surgiram, mas como a original, nenhuma delas havia sido confrontada empiricamente.

Metcalfe topou o desafio de visitar sua lei e fez uma interessante constatação. Primeiro, partiu de uma constatação evidente, que o valor das redes não cresce ao infinito como as formulações originais da sua lei e de outras similares sugerem. Então ele pensou em N como uma função no tempo e pegou dados reais, do Facebook, relativos aos 10 anos anteriores. No final de 2012, o Facebook tinha 1,06 bilhão de usuários e 150 bilhões de conexões entre amigos. Para estimar o crescimento de usuários do Facebook, Metcalfe generalizou uma curva senoide (que possui formato de S) utilizada para modelar crescimentos populacionais. A esta generalização, deu o



nome de “netoid”, que é definida da seguinte maneira:

A netoide tem a mesma forma de curva em S que o sigmóide. Sua inclinação (a taxa de adoção) é proporcional ao produto da fração da população que já adotou [o Facebook, no caso] vezes a fração que aguarda adoção. Ele atinge o pico quando a adoção é de 50%. A taxa de adoção é determinada pelo número de adoções até o momento e limitada pelo número de pessoas que aguardam adoção. O netoide oferece três parâmetros:  $h$ , o momento em que a taxa de crescimento é máxima, quando a população está na metade do pico;  $v$ , a viralidade ou velocidade com que a adoção ocorre; e  $p$ , o valor de pico, com o qual o netoide se aproxima assintoticamente. Em resumo, o netoide pode modelar quando e com que rapidez a adoção ocorrerá e qual será o tamanho<sup>19</sup>

Depois disso, Metcalfe plotou o crescimento do número de usuários do Facebook de 2004 a 2013, utilizando a média de usuários mensais, em bilhões. Em seguida, alinhou os parâmetros para ajustar os dados à curva e chegou em um valor de pico de 2,5 bilhões. Até aquele momento, o número de usuários do Facebook ainda não atingia a metade do pico, então sua taxa de crescimento ainda aumentava. Em seguida, plotou o faturamento do Facebook nos últimos 10 anos e ajustou os parâmetros para atender a função da Lei de Metcalfe e a curva se alinhou bem aos dados empíricos. A figura a seguir mostra os resultados obtidos. (METCALFE, 2013)

Em 2014, três pesquisadores chineses repetiram o processo de verificação, agora, com dados do Facebook e, também, com dados da Tencent, maior rede social da China. Os resultados confirmaram que a Lei de Metcalfe alinha-se bem aos números reais, considerando-se o faturamento das empresas e o número médio de usuários mensais. Segundo os pesquisadores: “Tencent e Facebook possuem grandes diferenças em termos de receita, custos<sup>20</sup>, modelos de negócio e tecnologia. Mesmo assim, a Lei de Metcalfe se alinha bem aos dados de ambas”<sup>21</sup>. (ZHANG; LIU; XU, 2015)

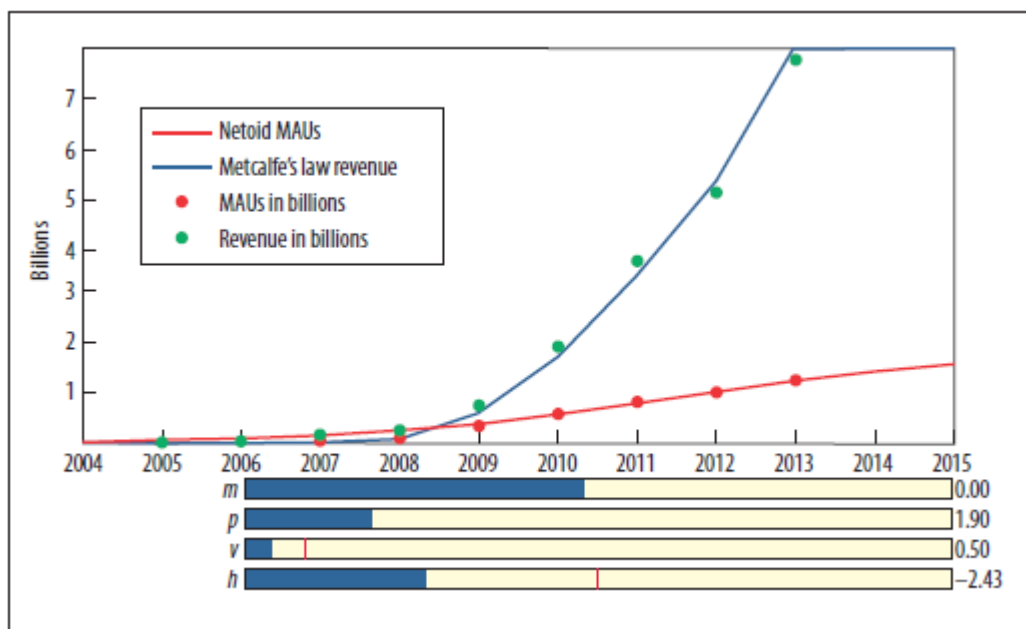
Mas qual é a relevância da Lei de Metcalfe para a discussão travada neste trabalho? A resposta está na conexão entre a curva de faturamento e a fonte de receita das plataformas. Se as plataformas fossem remuneradas diretamente pelos usuários, apenas em hipóteses muitíssimo improváveis - para não dizer impossíveis - a receita

<sup>19</sup> No original: “The netoid has the same S-curve shape as the sigmoid. Its slope (the adoption rate) is proportional to the product of the fraction of the population already adopted times the fraction awaiting adoption. It peaks when adoption is 50 percent. The adoption rate is driven by the number of adoptions so far and limited by the number of those awaiting adoption. The netoid offers three parameters:  $h$ , the point in time at which the growth rate is maximum, when the population is half the peak;  $v$ , the virality or speed with which adoption occurs; and  $p$ , the peak value, which the netoid approaches asymptotically. In short, the netoid can model when and how fast adoption will occur, and how large it will get.” (tradução deste mestrando)

<sup>20</sup> Neste trabalho, os pesquisadores também concluíram que o custo tem crescimento quadrático, mas adotaram uma definição muito simplista de custos, como equivalente ao total de receita menos o lucro líquido, abarcando nos custos, por exemplo, valores de investimentos. Essa decisão sobre a conceituação do custo pode tornar o resultado discutível.

<sup>21</sup> “Tencent and Facebook have big differences in revenue, cost, business model, and technology. Yet both of their actual data fit Metcalfe’s law well.” (tradução deste mestrando)

Figura 3 – A netoide se ajusta bem aos dados de crescimento de usuários do Facebook, medidos em termos de usuários médios mensais (MAUs), e a lei da Metcalfe se ajusta bem aos dados de receita do Facebook.



Fonte: Bob Metcalfe (2013)

creceria em ordem quadrática ( $V \sim N^2$ , onde  $V$  representa o faturamento e  $N$  o número de usuários). O comportamento natural seria um crescimento linear ( $V = c \cdot N$ ), onde  $c$  representa o valor de uma mensalidade mais um valor relativo à média de serviços adicionais adquiridos pelos usuários.

Assim, todo o efeito de rede observado na curva de crescimento da receita advém do modelo de negócio que traz a zero o valor pago pelo usuário. Desta forma, o valor zero tem um impacto econômico que vai muito além do efeito psicológico causado no usuário, que se sente atraído por uma oferta irresistível. Este valor especial também possibilita um efeito que acelera o crescimento da receita de modo muito mais contundente do que o modelo de remuneração direta, realizada em dinheiro pelo usuário, o que tende a aumentar a geração de excedente necessário para novos investimentos de expansão sem grandes sacrifícios à lucratividade, criando um ambiente ideal para aumento da capilaridade física e lógica, o investimento em novas tecnologias e a aquisição de empresas complementares ou concorrentes, de modo a consolidar um posicionamento dominante.

Neste sentido, criar mecanismos que aumentam a autonomia dos usuários com relação à disposição dos seus dados e, também, na interrupção da apresentação das mensagens publicitárias que, nunca é demais lembrar, nascem das próprias atividades executadas pelos usuários nas plataformas, ajuda não apenas na proteção do indiví-

duo, por ter mais controle dos seus dados pessoais, mas também pode aplacar em alguma medida a velocidade de crescimento de faturamento que, na casa das centenas de milhões ou de bilhões de usuários, favorece a consolidação de monopólios e gera situações de abuso de posição dominante que, em muitos casos, são difíceis de serem combatidos pelos métodos tradicionais de controle de comportamento anticoncorrencial.

### 3.2 PERSONALIDADE COMO MERCADORIA SEM PREÇO

A revista *The Economist*, na edição de 6 de maio de 2017, em sua matéria de capa dedicada à necessidade de revisão do sistema de regulamentação antitruste relacionado à economia de dados, abre o texto classificando-os como uma nova commodity: “o petróleo da era digital” (THE ECONOMIST, 2017).

Mas diferente do petróleo, que dorme silencioso sob a terra, o quantum de valor desta nova economia nos é imanente. São os rastros de nossos passos, os fluxos que nascem de nossas decisões, os pequenos fragmentos de informação que ajudam a formar o mosaico da personalidade humana. Os dados pessoais, verdadeiros ativos do ponto de vista econômico, são, sob a ótica dos direitos fundamentais, bens jurídicos de cuja tutela depende, em grande medida, a proteção da personalidade.

Como bem destaca Zuboff (2019), a frase “Quando você não paga, você é o produto” não é adequadamente aplicável para descrever a captação de dados pessoais. Neste caso, o usuário é um fornecedor de matéria-prima, uma posição muito bem representada pela metáfora exposta na capa de *The Economist*. Na verdade, o lema “você é o produto” tem um caráter redutor perigoso, porque negligencia as diversas posições simultâneas ocupadas pelos usuários destas plataformas. É possível pensar no usuário como produto, mas a partir de uma outra posição, quando se torna um alvo muito preciso para anunciantes que pagam por posições de anúncio gerados pelos próprios usuários no processo de uso das plataformas.

Esta seção cuidará, especificamente, da posição do usuário como um fornecedor de dados pessoais e quais os impactos deste posicionamento na proteção dos direitos da personalidade destes usuários, a partir da descrição do caráter duplo dos dados pessoais para então passar à sua proteção constitucional e a difícil e intrincada arquitetura jurídica necessária para conciliar, mesmo que ao custo de certa coerência, na prática, este duplo caráter dos dados pessoais.

#### 3.2.1 A dupla face dos dados pessoais e a sua proteção constitucional

No artigo de introdução do livro *“Brançosos” e Interconstitucionalidade, Itinerários do Discurso sobre a Historicidade Constitucional*, dedicado à apresentação dos grandes desafios do constitucionalismo no século XXI, J. J. Gomes Canotilho (2008)

faz uma afirmação corajosa: “É preciso navegar entre o *Estado de direito* e a *República constitucional comercial*, e compreender como a “fortuna” e a “virtude” se agitam no contexto de novas sociedades em rede”.

No final do mesmo livro, ao abrir a seção de artigos prospectivos, que tentam traçar perspectivas futuras para o constitucionalismo, Canotilho define precisamente a *República Comercial* como aquela onde

se mistura a ilusão de uma comunidade baseada na Internet, a pretensão de excelência assente na capacidade de governação transnacional de actores privados e a utopia de um constitucionalismo global estruturado em constitucionismos parciais civis (sem política).

No bojo da autocrítica sobre a Constituição dirigente, Canotilho dá luz ao contexto onde se trava a luta pela proteção dos dados pessoais como forma de garantir o exercício e o desenvolvimento máximo da personalidade e da liberdade. Máximo e não pleno, porque não é possível viabilizar categorias de completude. O agito de “fortuna” e da “virtude” na sociedade em rede passa necessariamente por entender o caráter duplo dos dados pessoais. Como as moedas que estampam as faces dos personagens, em Ubik, de um lado, um traço, uma pequena porção da própria personalidade, de outro, um valor de troca.

Mas como já abordado, a relação de troca explica muito parcialmente o complexo contexto de utilização dos dados pessoais pelos serviços digitais disponibilizados gratuitamente. A capacidade de manejar estas peças de mosaico<sup>22</sup>, rearranjando-as de forma a identificar um alvo adequado para uma mensagem publicitária, entregue a partir de um processo de leilão, e também utilizadas para aumentar o nível de eficiência para captura do tempo dos usuários, precisa ser considerada ao estabelecer-se os limites constitucionais de utilização dos dados pessoais.

Quanto à *República comercial*, a descrição de Canotilho não é menos precisa. A ilusão de um aldeia global não resistiu às bolhas nas quais as pessoas se fecham, em grande medida resultado da própria arquitetura da rede, estruturada para disseminar opiniões e conectar as pessoas e suas afinidades. A confiança nas estruturas e nos métodos de governança privados, além da transferência de boa parte das responsabilidades regulatórias para as próprias empresas reguladas, são traços claros da “pretensão de excelência assente na capacidade de governação transnacional de actores privados”, cuja legitimação é construída, no caso da formulação normativa sobre tecnologia da informação, com a participação dos próprios atores de mercado,

<sup>22</sup> “O efeito mosaico ocorre quando as informações em um *dataset* individual, isoladamente, podem não representar um risco de identificação de um indivíduo (ou ameaça a algum outro interesse importante, como segurança), mas quando combinadas com outras informações disponíveis, podem representar esse risco.” (UNITED STATES OF AMERICA, 2013). Texto original: “The mosaic effect occurs when the information in an individual dataset, in isolation, may not pose a risk of identifying an individual (or threatening some other important interest such as security), but when combined with other available information, could pose such risk.”

como deixa claro Cohen (2019), em uma realidade de dispersão de poder que não está mais firmemente concentrada nos governos e organizada em instituições políticas, mas que se multiplica em núcleos menores, menos visíveis, com forte atuação pela rede e que, muitas vezes, se legitimam por meio de um discurso de deslegitimação das instituições políticas tradicionais. Também neste ponto, a metáfora dos “brancos”, de Canotilho, é surpreendentemente eficaz.

Antes de abordar a eficácia da proteção constitucional dos dados pessoais, duas considerações devem ser feitas, para tornar as conclusões mais claras. Primeiro, é necessário entender a categoria jurídica do que está sendo tutelado, ou seja, do dado em si considerado. O segundo aspecto diz respeito à categoria da tutela.

### 3.2.1.1 Bens não rivais, propriedade e acesso

Há várias definições possíveis para o termo “dado”. A primeira premissa assumida, aqui, para a construção de uma definição, é a sinonímia entre dado e informação, o que não é feito por acaso ou capricho, mas por ter sido a decisão do legislador, no Brasil e na Europa, respectivamente: na LGPD (art. 5º, I, “informação relacionada a pessoa natural identificada ou identificável”) e na GDPR (Art. 4º, n.º 1, “«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»)...”). A segunda é a adoção de uma definição abrangente para o termo informação, mas estreitamente ligada ao meio digital, tendo em vista que o foco de estudo são os sistemas digitais, utilizados sem a necessidade de uma contrapartida pecuniária, por parte do usuário.

Para Shapiro e Varian (1999), informação é “qualquer coisa que possa ser digitalizada - codificada como um fluxo de bits”<sup>23</sup>. Neste sentido, qualquer conjunto de informações, como um livro digital, uma foto, um arquivo de áudio, um banco de dados estruturado, as mensagens de texto em um aplicativo de mensagens, os registros em uma *timeline* de uma rede social, um conjunto de e-mails ou o fluxo de navegação de uma pessoa, pode ser considerado um bem informacional (*information good*). Aproveitando a definição de Shapiro e Varian e complementando com o contexto normativo, chegamos à seguinte definição de *dado pessoal*: *qualquer coisa que possa ser digitalizada - codificada como um fluxo de bits - relativa a uma pessoa natural*. Da mesma forma, qualquer conjunto de dados pessoais também pode ser caracterizado como um bem informacional. Importante ter em mente que a proteção de dados pessoais abarca tanto dados digitais quanto aqueles suportados por meios físicos, portanto, uma definição mais específica mantém a coerência argumentativa, pois o conjunto delineado na definição está totalmente contido no conjunto dos dados pessoais, conforme definido pelas legislações específicas.

<sup>23</sup> No original: “anything that can be digitized—encoded as a stream of bits” (tradução livre)

Os bens informacionais são, essencialmente, não rivais. Isso significa que a utilização de um dado por uma pessoa não diminui ou reduz a sua disponibilidade para outros. Complementarmente ao seu caráter não rival, os dados também possuem um custo próximo a zero para replicação (cópia e distribuição). O mesmo não acontece com os bens materiais que são rivais, ou seja, neste caso a utilização por uma pessoa impede a utilização por outra ao mesmo tempo. Um carro ou um equipamento, como um celular ou um computador, são exemplos de bens rivais. O petróleo também é rival, já que depois de consumido por alguém há menos petróleo para ser consumido.

Posse e propriedade de bens rivais são, em geral, facilmente resolvidas, já que o domínio de um significa a exclusão da possibilidade de domínio do bem por todos os outros. Já para os dados, essa facilidade se dissolve. Seu caráter não rival e o baixo custo de replicação dos dados tornam os contornos rígidos da propriedade, como categoria jurídica, difíceis de serem aplicados, fazendo com que, muitas vezes, seja mais fácil manejar uma outra categoria para ordenar o seu fluxo: o acesso.

O regime de controle por acesso é, em grande medida, defendida pelas empresas que têm, no seu *core business*, o tratamento de dados. Hal Varian (2018) trata deste tema em artigo dedicado à análise das relações econômicas com a inteligência artificial e a organização industrial, defendendo a ideia de que o foco não deve ser definir quem detém a propriedade dos dados, mas quem pode, efetivamente, acessá-los. E dois grandes motivos sustentam a posição das empresas: primeiro porque muitas delas produzem dados e contam, ao mesmo tempo, com o acesso a dados de outros players. E segundo porque são claros os critérios a serem utilizados para definir quem pode se qualificar como o dono de um conjunto de dados (DREXL, 2016). Como já exposto no primeiro capítulo, as capilaridades lógica e física, bem como a integração entre diversos *player* e múltiplas plataformas dificulta, realmente, a atribuição de direitos de propriedade e torna muito complexo os mecanismos de controle sobre a existência ou não de tratamentos específicos, uma questão muito sensível quando se trata de proteção de dados pessoais.

Drexl (2016) coloca a questão em uma perspectiva bastante razoável:

Não existe uma lei natural que diga que os dados como um ativo, embora possam ter valor econômico, devam pertencer a alguém. Em vez disso, o reconhecimento de qualquer novo direito deve, como é o caso da propriedade intelectual em geral, ser considerado uma forma de regulamentação governamental do mercado, que necessita de uma justificativa específica. No que se refere a propriedade de dados, que permite a comercialização dos dados por seu proprietário, essa justificativa precisa ser econômica<sup>24</sup>.

<sup>24</sup> No original: "There is no natural law that says that data as an asset, although it may have economic value, has to be owned by anybody. Rather, recognition of any new right should, as is the case in intellectual property in general, be considered a form of government regulation of the market, which is in need of a particular justification. In terms of data ownership, which enables its owner to commercialise data, this justification needs to be an economic one." (tradução deste mestrando)

Neste sentido, a regulação deveria sempre levar em consideração a eficiência econômica, onde o grau de liberdade de circulação dos dados, como ativos, possui relevância predominante e as tentativas de limitar sua circulação deveriam ser encaradas como intervenções estatais no mercado. De modo mais específico, é importante levar em conta que a ideia de aplicação, aos dados pessoais, de mecanismos de proteção de propriedade intelectual não é nova. Remonta da década de 1970, com o trabalho pioneiro de Richard Posner (2010), que avaliou essa possibilidade e concluiu pela sua inviabilidade por considerar que os custos relacionados aos controles eram mais elevados do que o valor das informações a serem protegidas. Esta discussão sobre o custo é retomada, no âmbito das legislações de proteção de dados, como uma crítica contundente ao sistema de *notice and consent*, no qual estas legislações se baseiam, tendo em vista que os custos de verificação e fiscalização seriam maiores do que o valor do que está sendo protegido. (DUCH-BROWN; MARTENS; MUELLER-LANGER, 2017)

Esta crítica não é sem razão, principalmente se for considerada a complexa estrutura de dados necessária para disponibilizar os serviços digitais gratuitos, no formato em que são disponibilizados hoje. A tutela centrada amplamente no dado em si cria problemas de verificação realmente relevantes, tendo em vista que as externalidades percebidas não são capazes de explicitar eventuais tratamentos de dados fora de conformidade. Isso leva à necessidade de criação de mecanismos de avaliação que, como já abordado anteriormente, são muitas vezes delegados às próprias empresas. Modelos mais contundentes de fiscalização envolveriam, necessariamente, ações de auditoria e controle a serem realizadas dentro das empresas e que, mesmo assim, não garantiriam a descoberta de desvios relevantes em decorrência da imensa complexidade e capilaridade dos sistemas que sustentam estes serviços. Por este motivo, atuações nas bordas, criando mecanismos de limitação de captura de dados pessoais e também restringindo os resultados (*outputs*) indiretos podem ser alternativas viáveis para o aumento do nível de proteção dos titulares de dados pessoais.

A opção por um regime único, que compatibilize direitos de propriedade e acesso, também não é clara nos contornos legislativos, como acontece no caso europeu e, pela proximidade das legislações de proteção de dados, em grande medida também aplicável ao caso brasileiro. Duch-Brown, Martens e Mueller-Langer (2017), em relatório técnico produzido pelo Joint Research Centre, ligado à Comissão Europeia, sobre o tema, esclarecem:

A GDPR deliberadamente não considera direitos de propriedade, totais e transferíveis, para dados pessoais. Justifica a ausência de direitos de propriedade negociáveis sobre dados pessoais com base em argumentos de direitos humanos: a privacidade é um direito humano básico que não pode ser alienado. Cria direitos específicos inalienáveis e não negociáveis para pessoas naturais, incluindo (a) a proibição de processamento de dados sem uma base legal (por exemplo, "consentimento informado"), (b) a proibição de uso de

dados pessoais para outros fins alheios àqueles para os quais eles foram originalmente coletados, (c) o direito do titular dos dados de acessar e extrair ("portar") seus dados pessoais; e (d) o direito de ser esquecido<sup>25</sup>.

Complementam os autores, acertadamente, destacando que os dados coletados para um determinado fim podem ser alvo de tratamento para outras finalidades, desde que não sejam incompatíveis com o propósito original. Nitidamente, abre-se um amplo espectro interpretativo sobre o enquadramento de uma determinada atividade como não incompatível com a atividade que deu origem à coleta dos dados.

Há um entendimento, porém, que apesar de reconhecer que a GDPR não provê explicitamente um direito de propriedade, alguns aspectos deste direito podem e devem ser manejados pelos titulares de dados pessoais em determinadas circunstâncias. Boerding *et al.* (2018) identificam dois deles: o primeiro ligado ao exercício do direito de exclusão, também referenciado, no direito europeu como *direito ao esquecimento*. Neste caso, o titular tem o direito de solicitar e ter atendido seu pedido para apagamento dos dados pessoais relativos a ele, não em todas as circunstâncias, mas aplicável ao caso relevante de tratamento de dados pessoais tendo o consentimento como base legal. Visto sob uma outra ótica, argumentam os autores,

o indivíduo recebe um poder de disposição exclusiva referente ao processamento de dados pessoais que é - até certo ponto - comparável ao poder do proprietário sobre sua propriedade. Em termos de direito de propriedade, isso pode ser entendido como uma dimensão negativa de um direito exclusivo, ou seja, o poder de excluir outras pessoas do uso da propriedade<sup>26</sup>.

O segundo refere-se ao *direito de portabilidade* dos dados pessoais, onde o titular tem o direito de receber os dados pessoais que lhe digam respeito de um controlador em um formato em que os dados possam ser utilizado e processado por computador e de transferi-los para outro controlador sem que o controlador original possa impedi-lo. Para os autores (BOERDING *et al.*, 2018), este é mais exemplo de direito que não se liga a paradigmas originais de proteção de dados pessoais, como no caso clássico do consentimento, mas de um direito baseado no conceito de propriedade.

Os autores concluem, para o caso específico dos dados pessoais, que a propriedade dos dados deve ser alocada com os titulares, ficando o controlador como detentor

<sup>25</sup> No original: "The GDPR deliberately does not consider full and transferable private ownership rights for personal data. It justifies the absence of tradable ownership rights in personal data on the basis of human rights arguments: privacy is a basic human right that cannot be alienated. It creates inalienable and non-tradable specific rights for natural persons including (a) the prohibition of data processing without a legal basis (e.g. "informed consent"), (b) the prohibition to use personal data for other purposes than those for which they were originally collected, (c) the right for the data subject to access and extract ("port") his personal data, and (d) the right to be forgotten."

<sup>26</sup> No original: "the individual is granted a power of exclusive disposition concerning the processing of personal data that is—to some extent—comparable with the power of the owner over his property. In terms of property law, this could be understood as a negative dimension of an exclusive right, i.e., the power to exclude others from using one's property." (tradução deste mestrando)



de direitos limitados de coleta, uso e transmissão dos dados (BOERDING *et al.*, 2018). Apesar de valorosa, a proposta enfrenta obstáculos relevantes, principalmente pelo fato de que as circunstâncias onde o titular dos dados poderia exercer estes direitos de propriedade são, na verdade, situações excepcionais e aplicáveis não a todo o seu acervo de dados sob a guarda de um determinado controlador, mas apenas a uma parte que pode ser mais ou menos representativa, a depender do tipo de relação existente entre titular e controlador. Neste ponto, considerando o contexto normativo europeu extensível ao Brasil com a LGPD, a pergunta ‘*De quem são os dados?*’ não faz muito sentido.

Para os dados pessoais tratados pelas plataformas digitais gratuitas, exclusivamente no âmbito do Direito Europeu, a aprovação da Diretiva 2019/770, que trata de aspectos relativos ao fornecimento de conteúdos e serviços digitais, traz luz ao tema, dando maior segurança jurídica para as empresas, ao legitimar o fornecimento de dados pessoais como contrapartida não pecuniária ao fornecimento dos serviços, já no Artigo 3.º, n.º 1 (grifo nosso):

A presente diretiva é aplicável a qualquer contrato em que o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e o consumidor pague ou se comprometa a pagar o respetivo preço.

*A presente diretiva é igualmente aplicável sempre que o profissional forneça ou se comprometa a fornecer conteúdos ou serviços digitais ao consumidor e o consumidor faculte ou se comprometa a facultar dados pessoais ao profissional, exceto se os dados pessoais facultados pelo consumidor forem exclusivamente tratados pelo profissional para fornecer os conteúdos ou serviços digitais em conformidade com a presente diretiva, ou para o profissional cumprir os requisitos legais a que está sujeito, não procedendo ao tratamento desses dados para quaisquer outros fins.*<sup>27</sup>

O texto do artigo não deixa absolutamente claro o caráter transacional do fornecimento dos dados pessoais como contrapartida pela prestação de serviços ou disponibilização de conteúdos digitais. Esta explicitação, mesmo com o manejo de certo eufemismo, acontece no Considerando número 24 da Diretiva:

(24) | Os conteúdos ou serviços digitais são, além disso, frequentemente fornecidos em situações em que o consumidor não paga um preço, mas faculta dados ao operador. Esses modelos de negócios específicos aplicam-se já de diferentes formas numa parte considerável do mercado. Embora reconhecendo plenamente que a proteção dos dados pessoais é um direito fundamental e que, por conseguinte, os dados pessoais não podem ser considerados

<sup>27</sup> Texto extraído da versão em português, de Portugal, da diretiva. A seguir, apresenta-se o texto equivalente na versão em inglês: “Article 3. Scope. 1. This Directive shall apply to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price. This Directive shall also apply where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.”

um produto de base [*commodity*], a presente diretiva deverá assegurar que os consumidores gozem, no contexto desses modelos de negócio, do direito a meios de ressarcimento ao abrigo do contrato. Por conseguinte, a presente diretiva deverá ser aplicável aos contratos em que o profissional fornece ou se compromete a fornecer conteúdos digitais ou a prestar serviços digitais ao consumidor e este fornece ou compromete-se a facultar dados pessoais. Os dados pessoais podem ser facultados ao profissional no momento em que o contrato é celebrado ou posteriormente, como nos casos em que o consumidor dá o seu consentimento para que o profissional utilize os dados pessoais eventualmente carregados ou criados pelo consumidor no âmbito da utilização dos conteúdos ou serviços digitais.<sup>28</sup>

O caráter complementar à GDPR, com prevalência da norma de proteção de dados pessoais em casos de conflito, fica evidente na dicção do mesmo art. 3.º, em seu item 8, ao declarar que que “a presente diretiva não prejudica o Regulamento (UE) 2016/679 e a Diretiva 2002/58/CE. Em caso de conflito entre as disposições da presente diretiva e o direito da União em matéria de proteção de dados pessoais, prevalece este último”. A implicação mais relevante, neste caso, relaciona-se com a necessidade da existência de uma base legal de tratamento, dentre aquelas estabelecidas na GDPR, mesmo para os dados utilizados como contrapartida pela prestação dos serviços, posição à qual se alinha Maria de Almeida Alves (2019). Como se pode notar, mesmo com a nova diretiva, ainda permanece a controvérsia sobre a possibilidade de se considerar os dados pessoais como bens comercializáveis (alinhando-se ao direito de propriedade) ou a vedação desta possibilidade, com base na inalienabilidade dos direitos da personalidade.

Após a aprovação da Diretiva 2019/770, a EDPB emitiu um documento com *Guidelines* sobre o tratamento de dados pessoais com base no artigo 6(1)(b), da GDPR, ou seja, a base legal que autoriza o tratamento para execução de um contrato no qual o titular é parte. Ao tratar do processamento de dados pessoais para melhoria dos serviços, o EDPB sinaliza que, no caso geral, os tratamentos não podem ser respaldados por esta base legal, mas abre espaço para a consideração de outras hipóteses como o legítimo interesse e o consentimento. Já na abordagem do processamento para publicidade comportamental online, o EDPB é mais contundente. Declara que este tipo de operação de tratamento, associado com rastreamento e perfilização dos titulares de dados, é muitas vezes usado para financiar serviços online e que, na regra

<sup>28</sup> Versão do texto da Diretiva em inglês: “Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service.”

geral, estes processamentos não são necessários diretamente para a execução do contrato de serviços online. Em seguida, assevera:

O artigo 6.o, n.o 1, alínea b), não pode fornecer uma base legal para a publicidade comportamental simplesmente porque essa publicidade indiretamente financia a prestação do serviço. Embora esse processamento possa suportar a entrega de um serviço, isso por si só não é suficiente para estabelecer que é necessário para a execução do contrato em questão.

(...) Considerando que a proteção de dados é um direito fundamental garantido pelo Artigo 8 da Carta dos Direitos Fundamentais, e levando em conta que um dos principais objetivos da GDPR é fornecer aos titulares de dados controle sobre as informações a eles relacionadas, os dados pessoais não podem ser considerados uma mercadoria negociável [tradeable commodity]. Mesmo se o titular dos dados puder concordar com o processamento de dados pessoais, ele não poderá trocar seus direitos fundamentais por meio deste contrato<sup>29</sup>.

Neste ponto, a confirmação dos dados pessoais como contrapartida legítima para prestações de serviços digitais, como estabelecido na Diretiva 2019/770, mantém relevante as considerações de Cohen (2019) sobre a forma como os textos normativos vão sendo moldados para encaixarem-se nos modelos de negócio dominantes, o que demonstra o caráter ativo destas organizações, resultado de um esforço de criar um ambiente normativo adequado aos negócios e não um ambiente sem regulação como pode parecer à primeira vista.

O caráter indefinido do dado, que hora pode ser protegido por mecanismos de propriedade, principalmente depois de atividades de processamento, e hora devem ser vistos sob o prisma do acesso, especificamente quanto aos dados brutos que servem de matéria-prima para grandes operações de processamento de dados, também se alinha à perspectiva traçada por Cohen (2018), ao considerar esse arranjo favorável às empresas. A conclusão de Drexler (2016) ajuda a esclarecer que esta situação de indefinição é, na verdade, uma opção agradável às empresas:

Em princípio, na economia de dados, não são necessários incentivos para gerar e comercializar dados. Os detentores de dados podem cobrar um preço pela disponibilização de dados a terceiros, com base no controle factual dos dados, apoiado por medidas técnicas de proteção<sup>30</sup>

Uma grande lição pode ser extraída do caso europeu. A falta de um estatuto claro, que equilibre propriedade e acesso, combinado com a constatação fática de que

<sup>29</sup> No original: “Article 6(1)(b) cannot provide a lawful basis for online behavioural advertising simply because such advertising indirectly funds the provision of the service. Although such processing may support the delivery of a service, this in itself is not sufficient to establish that it is necessary for the performance of the contract at issue. (...) Considering that data protection is a fundamental right guaranteed by Article 8 of the Charter of Fundamental Rights, and taking into account that one of the main purposes of the GDPR is to provide data subjects with control over information relating to them, personal data cannot be considered as a tradeable commodity. Even if the data subject can agree to the processing of personal data, they cannot trade away their fundamental rights through this agreement.” (tradução livre)

<sup>30</sup> No original: “In principle, in the data economy, no incentives are needed for generating and commercialising data. Data holders are able to charge a price for making data available to third parties based on factual control over data, supported by technical protection measures.” (tradução livre)

os usuários estão inseridos no mercado de dados, situação reconhecida na Europa a partir da aprovação da Diretiva 2019/770, e com as limitações de um sistema de proteção muito baseado no "*notice and consent*" exige a busca de novas alternativas para garantir o pleno exercício dos direitos de personalidades dos titulares de dados pessoais.

### 3.2.1.2 Proteção de dados pessoais como garantia constitucional

A Proposta de Emenda à Constituição (PEC) número 17, de 2019, em adiantado trâmite no Congresso Nacional, no momento em que este trabalho é escrito, inclui o inciso LXXIX ao art. 5o, da Constituição Federal, para tornar explícita a proteção dos dados pessoais no rol de Direitos Fundamentais, com a seguinte redação:

LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

Importante notar, neste ponto, que nas diversas idas e vindas do texto em seu trâmite legislativo, decorrentes, algumas vezes, não da inclusão explícita da proteção de dados pessoais como Direito Fundamental, mas por questões de ordem mais prática como, por exemplo, a fixação, em texto constitucional, da obrigatoriedade de instalação de um órgão regulador, na LGPD designado por Autoridade Nacional de Proteção de Dados, que seja "independente, integrante da administração pública federal indireta, submetida a regime autárquico especial", houve variações, também, na forma de disposição do direito à proteção de dados pessoais no texto constitucional.

A versão apresentada acima consta em texto substitutivo adotado, em 10 de dezembro de 2019, pela Comissão Especial da Câmara para proferir parecer sobre a PEC 17/2019. Esta mesma redação aparece no relatório do Dep. Orlando Silva (PCdoB-SP), apresentado na mesma Comissão, no dia 04 de dezembro de 2019. Já a versão original da PEC 17/2019, protocolado em 12 de março de 2019, propunha a inclusão do inciso XII-A, com a mesma redação do substitutivo de dezembro. Já o texto remetido pelo Senado à Câmara dos Deputados, em 3 de julho de 2019, não continha a previsão de criação de mais um inciso, mas sim a alteração do próprio inciso XII, nos seguintes termos:

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;

Apesar de parecer mera filigrana textualística ou excesso de preciosismo no trato do texto legal, esse posicionamento revela - ou pode esconder, caso decida-se pela redação em inciso independente - um aspecto essencial na formulação do Direito

Fundamental à proteção de dados pessoais. Está-se diante de um direito, em sentido estrito, ou diante de uma garantia constitucional?

A doutrina cria linhas marcantes que separam direitos e garantias, no âmbito do Direito Constitucional. Paulo Bonavides (2013) reproduz estes contornos traçados por Jorge Miranda que, depois de mostrar as diferenças, posiciona direitos de liberdade e garantias (grifo no original):

Os direitos representam só por si certos bens, as garantias destinam-se a assegurar a fruição desses bens; os direitos são principais, as garantias acessórias e, muitas delas, adjetivas (ainda que possam ser objeto de um regime constitucional substantivo); os direitos permitem a realização das pessoas e inserem-se direta e imediatamente, por isso, nas respectivas esferas jurídicas, as garantias só nelas se projetam pelo nexos que possuem com os direitos; na acepção jusracionalista inicial, os direitos *declaram-se*, as *garantias estabelecem-se*. (...) As liberdades valem por aquilo que vale a pessoa, as garantias têm valor instrumental e derivado.

Não é por acaso, portanto, que se tenha inicialmente pensado em inserir o “direito à proteção dos dados pessoais” em um inciso imediatamente abaixo ou, em um segundo momento, no próprio inciso XII, do art. 5º da Constituição Federal, expressando um “direito à proteção” e não fazendo uma declaração dos direitos do indivíduo sobre os dados pessoais que lhe digam respeito. Claramente, a inovação constitucional proposta trata-se de uma garantia. O posicionamento, ao redor do inciso XII, revelaria ainda mais claramente estar-se falando de um Direito à Segurança, na classificação das garantias proposta por José Afonso da Silva (1994). Seria possível, então, falar-se em “segurança dos dados pessoais”

Aqui, neste ponto, importante fazer uma revisão histórica da previsão constitucional do reconhecimento de direitos individuais sobre dados pessoais na Constituição de 1988. Apesar de ser sólida a ideia de que o *habeas data* foi concebido como uma reação às experiências autoritárias vividas pelos países da América Latina, no momento de elaboração de suas novas Cartas Constitucionais (DONEDA, 2019), configurando-se assim como um olhar para o passado, o texto original, proposto por José Afonso da Silva à Comissão Provisória de Estudos Constitucionais (Comissão Afonso Arinos) tinha configurações claras de declaração de direitos relativos aos dados pessoais, como se observa nos artigos 17 e 31 do anteprojeto (SILVA, 1994):

#### Artigo 17

1. Toda pessoa tem direito de acesso aos informes a seu respeito registrados por entidades públicas ou particulares, podendo exigir a retificação de dados, e a sua atualização.
2. É vedado o acesso de terceiros a esses registros.
3. Os informes não poderão ser utilizados para tratamento de dados referentes a convicção filosóficas ou políticas, filiação partidária ou sindical, fé religiosa ou vida privada, salvo quando se tratar do processamento de dados estatísticos não individualmente identificáveis.

4. Lei federal definirá quem pode manter registros informáticos, os respectivos fins e conteúdos.

(...)

Artigo. 31

Conceder-se-á *habeas data* para proteger o direito à intimidade contra abusos de registros informáticos públicos e privados.

Declara-se, explicitamente, os direitos de acesso, retificação e atualização. Há referência textual aos registros informáticos. Os dados não se restringem àqueles mantidos em bancos de dados públicos, mas aos acervos de dados mantidos por entidades públicas e particulares. Há restrições claras ao tratamento de dados pessoais sensíveis, em uma acepção que seria razoável na década de 1980. Consta previsão de uso anonimizado de dados. E fixa a necessidade de Lei federal para regulação dos contornos da utilização de dados pessoais.

Como bem destaca José Afonso da Silva (1994), até o texto apresentado pela Comissão, que fez ajustes no trecho sobre o remédio constitucional, posicionando-o no artigo 48, direito e garantia andavam juntos. A partir deste momento, o texto foi reformado para pior, com a supressão do direito explícito e a manutenção da garantia processual.

A boa redação de Direitos Fundamentais relacionada a dados pessoais passa, necessariamente, por uma declaração de direitos, não apenas à menção de uma garantia, como a sua proteção. É assim, por exemplo, na Carta dos Direitos Fundamentais da União Europeia, que estabelece, no seu artigo 8.º:

Artigo 8.º

1. Todas as pessoas têm o direito à protecção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Importante notar que este artigo pertence ao Capítulo II da Carta de Direitos Fundamentais da União Europeia, que trata das Liberdades, bastante em linha, apesar do artigo não se restringir aos dados pessoais em meio digital, com a ideia de “liberdade informática” estabelecida por Vittorio Frosini, que a define nos seguintes termos:

Também a liberdade informática, como já foi dito sobre a liberdade política, tem dois lados. Um lado é o negativo, ou seja, o direito de não tornar públicas determinadas informações pessoais, privadas e confidenciais (essas qualificações, que em alguns casos podem não coincidir). O outro lado é o “positivo”, ou seja, exercer o direito de controle sobre os dados relativos à própria pessoa que já escapou do círculo de privacidade para se tornar elementos de entrada de um programa eletrônico; e, portanto, liberdade informática positiva

ou direito subjetivo reconhecido de conhecer, corrigir, remover ou adicionar dados em um formulário pessoal eletrônico.

Desse ponto de vista metodológico, pode-se apreender uma correspondência de simetria com o "direito à informação", que encontra seu limite, ou melhor, seu antagonista, no "direito ao sigilo", uma vez que aquele representa o inverso deste. No caso da liberdade informática, os dois aspectos, negativo e positivo, são complementares: desde que o exercício do direito consista precisamente no direito de intervir na composição dos dados, não apenas para limitar seu uso, proibindo o acesso de outros, mas também para executar uma tarefa de inspeção ou cancelamento, que corresponde ao direito de retificação das informações da imprensa e da televisão<sup>31</sup>.

A complementariedade dos aspectos positivo e negativo preenche a dimensão do controle do indivíduo sobre os dados que lhe dizem respeito, sendo esta a base do que Frosini designa de "liberdade informática" que, por sua vez, se alinha de modo preciso à evolução do sigilo ao controle, preconizada por Rodotà (2008) e que está na raiz do Direito à Autodeterminação Informativa, definido pelo Tribunal Constitucional Federal da Alemanha como "o direito dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados" (RUARO; RODRIGUEZ, 2010). Portanto, no centro dos direitos individuais relativos aos dados pessoais ou, para tornar a designação mais breve, no centro da liberdade informática está o controle. Nestes termos, fazendo uma leitura atual do termo, liberdade informática poderia ser definida como o direito do indivíduo de decidir a maneira como seus diversos acervos informacionais são utilizados.

Retornando à declaração dos direitos do artigo 8.º, da Carta de Direitos Fundamentais da União Europeia, o controle se expressa, essencialmente, como consentimento. Neste passo, todas as outras hipóteses autorizadoras de tratamento de dados pessoais, do ponto de vista dos Direitos Fundamentais, são excepcionalidades ou, visto do âmbito da eficácia, são limitadoras do Direito Fundamental ao controle sobre os próprios dados. Exatamente por isso, há a necessidade de autorização explícita, na Carta de Direitos Fundamentais, para impor-lhe restrição, desde que esta restrição esteja prevista em lei.

<sup>31</sup> No original: "Anche la libertà informatica, come è stato detto di quella politica, ha due facce. Una faccia è quella negativa, e cioè il diritto di non rendere di dominio pubblico certe informazioni di carattere personale, privato, riservato (qualifiche queste, che potrebbero in certi casi non coincidere tra loro). L'altra faccia è quella «positiva», di esercitare cioè un diritto di controllo sui dati concernenti la propria persona che sono già fuoriusciti dalla cerchia della privacy per essere divenuti elementi di input di un programma elettronico; e dunque libertà informatica positiva, o diritto soggettivo riconosciuto, di conoscere, di correggere, di togliere o di aggiungere dati in una scheda personale elettronica. Si potrebbe cogliere, sotto questo profilo metodologico, una corrispondenza di simmetria con il «diritto all'informazione», il quale trova nel «diritto al segreto» il suo limite, o meglio il suo antagonista, giacché l'uno rappresenta l'inverso dell'altro. Nel caso della libertà informatica, i due aspetti, negativo e positivo, si presentano come complementari fra loro: giacché l'esercizio del diritto consiste precisamente nella facoltà di intervenire sulla composizione dei dati non solo per limitarne l'uso vietandone l'accesso ad altri, ma anche per svolgere un compito ispettivo di verifica o di cancellazione, che corrisponde al diritto di rettifica per l'informazione a stampa e televisiva."

Traçar esse cenário mais amplo é necessário, não apenas para pontuar que, mais uma vez, o Brasil está próximo de perder uma oportunidade de inserir, no rol de Direitos Fundamentais, uma adequada declaração de direitos individuais ligados aos dados pessoais, mas principalmente por ser necessário dar consistência a esses direitos para, só então, definir a real abrangência da previsão constitucional de proteção dos dados pessoais como garantia.

Antes disso, ainda, é preciso considerar que o alinhamento entre consentimento e controle, como ocorre na prática, no direito europeu e, por ricochete, no texto da LGPD, obviamente diminui a esfera de controle do próprio indivíduo sobre os seus dados pessoais, já que não lhe permite, ao menos formalmente, a cessão dos seus dados pessoais como contrapartida por outro tipo de vantagem, como efetivamente ocorre na prática. Ao transformar o controle, na sua transposição para os textos normativos e para as declarações de Direitos Fundamentais, em consentimento, enfatizando seu caráter de composição da própria personalidade e negligenciando por completo sua face de bem economicamente apreciável, criou-se um arcabouço jurídico praticamente incompatível com a realidade, como ficou demonstrado na clara impossibilidade de compatibilização da GDPR com a Diretiva 2019/770, analisada na Seção 3.2.1.1. Na prática, os dados pessoais são usados como contrapartida para o acesso a serviços, como acontece no caso das plataformas digitais utilizadas sem contrapartida financeira por parte do usuário. Portanto, em certa medida, os dados pessoais configuram-se como um produto, mas há um impedimento, da ordem dos Direitos Fundamentais, para que lhes seja atribuído um preço.

Retornando ao “direito à proteção dos dados pessoais”, pode-se observar outra vantagem na separação do direito, em sentido estrito, ou seja, da liberdade informacional, da garantia constitucional. O caráter instrumental da proteção de dados pessoais como uma garantia permite a irradiação de seu efeitos para além da proteção da liberdade informática, entendida como o direito de controle, pelo indivíduo, sobre o uso do seu acervo informacional, atingindo todo o espectro das liberdades individuais. Assim, a proteção aos dados pessoais permite justificar a vedação do tratamento de dados pessoais com fins flagrantemente discriminatórios, mesmo que a operação de tratamento tenha sido autorizada pelo titular; estabelecer limites ao Estado no estabelecimento de mecanismos de vigilância; dar ao indivíduo o direito de solicitação de revisão de decisões automatizadas; tratar como ilegal a utilização de dados armazenados em dispositivos informáticos de uso pessoal sem autorização judicial específica.

Também permite a dissociação entre “proteção dos dados pessoais” e privacidade, tendo em vista que a garantia atinge o direito de liberdade (no caso, a privacidade), mas também o ultrapassa, garantindo ao indivíduo, por exemplo, o direito à portabilidade de seus dados pessoais, direito este que não se liga, de forma alguma, à privacidade, mas que se encaixa perfeitamente na garantia de controle sobre o acervo



de dados pessoais do indivíduo, portanto, dentro do âmbito da liberdade informacional.

A separação, no âmbito jurídico, entre privacidade e proteção de dados pessoais, como direito, em sentido estrito, e garantia, respectivamente, também ajuda a desembaraçar um aspecto econômico relevante: como bem a ser tutelado, privacidade se encaixaria mais claramente como um bem final, já ao posicionar a proteção como uma garantia, os dados pessoais seriam melhor enquadrados como bens intermediários.

Estas distinções estão muito longe de serem absorvidas pelos tomadores de decisão sobre a forma de uso dos dados pessoais, ou seja, pelos próprios indivíduos, no contexto de utilização das plataformas digitais. Também não são consensuais na doutrina e na jurisprudência. Contudo, este trabalho se propõe a sugerir uma nova forma de regulação para o uso dos dados pessoais, no âmbito específico das plataformas digitais, a partir vedação da gratuidade compulsória. Neste sentido, é fundamental que o formulador de política estabeleça claramente quais são os parâmetros conceituais utilizados na regulação sugerida. E o delineamento claro da separação entre os direitos relacionados aos dados pessoais e a garantia de proteção dos dados pessoais é parte essencial da sugestão apresentada no próximo capítulo.

### 3.3 CONSUMIDOR EMPACOTADO E ENTREGUE

A famosa máxima "os dados são o novo petróleo" guarda em si muitas contradições. A primeira delas tem relação com o caráter não rival dos dados, conforme já discutido na Seção 3.2.1. A segunda diferença elementar relaciona-se com o caráter ilimitado dos dados pessoais, em contraposição à quantidade finita de petróleo disponível. E a terceira e mais importante, sob a ótica deste trabalho, parte da origem e natureza do bem, já que não se pode esquecer que os dados pessoais são, potencialmente, parte da personalidade dos seus titulares.

Mesmo com todas essas diferenças, como ressalta Varian (VARIAN, 2019), dados são como o petróleo em um aspecto: precisam ser refinados antes de serem usados. E explica, em um artigo sobre concentração, competição e barreiras de entrada:

O processo de refino de dados requer matéria-prima (dados), capital (computadores e software) e mão-de-obra (analistas de dados). Como todos os fatores de produção, esses fatores exibem retornos decrescentes. O problema com a maioria das empresas não é que elas tenham poucos dados, mas que tenham tantos dados que é difícil organizá-los, gerenciá-los e analisá-los de maneira eficaz. O crescimento da computação em nuvem fará uma grande diferença aqui, já que hardware e software sofisticados agora estão acessíveis a todos. Atualmente, o maior desafio para as empresas que desejam implementar análise de dados é adquirir pessoas<sup>32</sup> (*acquiring people*) com as

<sup>32</sup> As questões relacionadas a atração de pessoas com *skill* adequado também pode ser encarada, em certa medida, como uma questão de capital. Um exemplo disso são os casos de *acqui-hiring*, quando a aquisição de uma empresa por outra é motivada, essencialmente, pela absorção dos seus

habilidades necessárias<sup>33</sup>.

Para ilustrar a questão relativa à curva de retorno decrescente dos dados como fator de produção, Varian apresenta um gráfico, em escala logarítmica, onde a taxa de erro, em sistemas de *machine learning*, cai linearmente com o incremento do volume de dados utilizados como base de treinamento, o que indica redução da escala de retorno dos dados. Nos experimentos elaborados por Hestness *et al.* (2017), todos da Baidu Research, braço de pesquisa em inteligência artificial da gigante de tecnologia chinesa Baidu, dona de um sistema de busca bastante popular na China, observa-se, realmente, um incremento da necessidade de dados para evolução dos resultados (diminuição da taxa de erro) numa escala que permite sugerir um retorno decrescente. Dito de outra forma, como demonstra o esboço resumo apresentado pelo estudo, quanto mais próximo da área de erro irreduzível (um limite testado apenas em problemas amostras, pelos autores, onde independente do volume de dados utilizados não haveria mais diminuição da taxa de erro) um maior volume de dados é necessários para gerar uma incremento na acurácia da aplicação, resultando numa diminuição da taxa de erro.

Mas as evidências empíricas apresentadas nesta pesquisa se restringem a aplicações específicas de *machine learning*, em especial tradução automática neural, modelos de linguagem, classificação de imagens e reconhecimento de voz (voz para texto ou *speech to text*). A extrapolação da lei de potência observada empiricamente, nestes experimentos, para todos os casos é arriscada. De todo modo, seguindo com a ampliação proposta por Varian, como traduzir esse resultado para o processamento dos dados pessoais por serviços digitais disponibilizados gratuitamente, no processo de apresentação dos anúncios para os usuários?

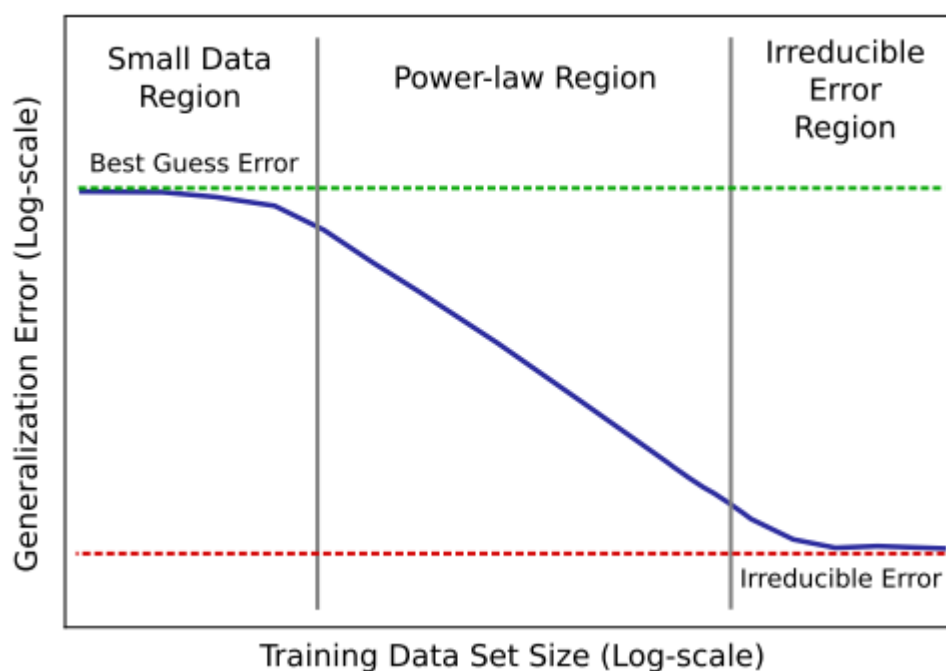
Considerando que estas aplicações buscam entregar aos anunciantes um perfil exato de consumidor e também o ajuda a ajustar a mensagem a ser endereçada para usuário alvo, a acurácia próxima da área irreduzível de erro seria aquela mais próxima possível do “mercado de um”, onde um produto altamente especializado poderia ser vendido pelo preço especializado mais alto, em uma estratégia de discriminação de preço de primeiro grau. O próprio Varian (2004), na primeira década do século, já identificava o uso da personalização pelos sistemas digitais gratuitos, mais especificamente pelos serviços de busca e já considerava crítica a utilização dos dados pessoais, mesmo que não considerasse esta uma questão ligada a privacidade:

---

profissionais. No Brasil a prática já acontece, como foi o caso da primeira aquisição realizada pelo Nubank ((CAPELAS, 2020))

<sup>33</sup> Texto original: "The process of refining data requires the raw material (data), capital (computers and software), and labor (data analysts). Like all factors of production, these factors exhibit decreasing returns. The problem with most companies is not that they have too little data, but that they have so much data that it is challenging to organize, manage, and analyze it effectively. The growth of cloud computing will make a big difference here, since sophisticated hardware and software is now accessible to everyone. The biggest challenge these days for firms that want to implement data analytics is acquiring people with the necessary skills." (tradução deste mestrando)

Figura 4 – Desenho esquemático da relação geral entre erro e volume de dados utilizados no treinamento de aplicações de inteligência artificial.



Fonte: Hestness *et al* (2017)

Obviamente, posso querer que meu alfaiate, meu médico e meu contador entendam minhas necessidades e me forneçam serviços personalizados. No entanto, é igualmente óbvio que, em geral, não quero que compartilhem essas informações com terceiros, pelo menos sem o meu consentimento. O problema não é a privacidade em si, mas a confiança: os consumidores querem controlar como as informações sobre si mesmos são usadas<sup>34</sup>

Continuando a aplicação da ideia de retornos decrescentes para os dados como fator de produção (matéria-prima), proposta por Varian e justificada pelos resultados obtidos nos experimentos de *machine learning*, aos dados pessoais utilizados pelos sistemas digitais gratuitos, chega-se à conclusão de que, quanto mais eficiente é a plataforma na realização do encontro entre o usuário alvo e o anunciante, maior a quantidade relativa de dados necessária para aumentar a acurácia, ou seja, um volume ainda maior de dados pessoais precisariam ser capturados e processados (poder computacional) por softwares cada vez melhores, criados por engenheiros e analistas de dados. Novos pontos de captura passam a ser necessários. As estruturas de capilaridade lógica e física precisam funcionar para que mais dados sejam gerados

<sup>34</sup> Texto original: "Obviously, I may want my tailor, my doctor, and my accountant to understand my needs and provide me with customized services. However, it is equally obvious that I do not, in general, want them to share this information with third parties, at least without my consent. The issue is not privacy per se, but rather trust: consumers want to control how information about themselves is used." (tradução deste mestrando)

e novas oportunidades de exposição de anúncios sejam criadas, já que o “encontro” pode ser otimizado por fatores temporais e geográficos. Assim, a *economia do encontro* faz nascer a *economia da vigilância*.

#### 4 DESARMANDO A ARMADILHA DA GRATUIDADE ENGANOSA

Plataformas digitais disponibilizadas sem contrapartida financeira por parte dos usuários finais, como apresentado no Capítulo 2, articulam quatro elementos fundamentais: (a) grande poder computacional, construído por arquiteturas complexas de processamento que podem ser operadas como estruturas únicas, conectadas a um número infindável de pontos de captura de dados em monstruosas teias de capilaridade lógica, que se estendem a partir da utilização de componentes de software distribuídos com código aberto (*open source*), serviços de software complexos utilizados via APIs e *embed codes*, todos embarcados em múltiplas aplicações e sites, além da capilaridade física, que capta dados a partir de sensores, câmeras e dispositivos que, cada vez mais, nos cercam e que tendem a se expandir a uma grande velocidade com o avanço da IoT; (b) apropriação do tempo dos usuários, de uma forma multidimensional, já que os motores de captação de dados pessoais funcionam de modo contínuo, não apenas enquanto estamos diretamente conectados à plataforma, mas por praticamente todo o tempo, aproveitando-se das teias de capilaridade física e lógica que capturam dados com potencial de serem direta ou indiretamente associados aos usuários, além da alocação do tempo dos usuários para criação das oportunidades de exposição publicitária, pois os espaços publicitários são criados dentro do processo de utilização da plataforma a partir do uso; (c) conteúdos dos outros, que são processados, reestruturados e entregues aos usuários sem nenhuma remuneração direta para o criador do conteúdo original, o que viabiliza a disponibilização de serviços com custos marginais muito próximos de zero; (d) dados pessoais que são fornecidos, como matéria-prima, para que as aplicações possam entregar, do outro lado da plataforma, a publicidade mais segmentada possível, maximizando as chances do anunciante converter uma venda.

Toda esta estrutura coloca o indivíduo que utiliza essas aplicações em três posições simultâneas, detalhadas no Capítulo 3. Operando em um processo circular, ele ao mesmo tempo é consumidor de um serviço ou conteúdo; fornecedor da matéria-prima fundamental para monetizar, em uma escala não linear (no caso do Facebook, por exemplo, uma escala quadrática), um complexo conjunto de serviços e, finalmente, como alvo da publicidade segmentada, posicionando-se como produto para a relação estabelecida entre a plataforma e o anunciante.

Esse arranjo, possível graças às características peculiares do ambiente digital, viabiliza uma acumulação de externalidades positivas, do ponto de vista das plataformas, que por alguns autores - Stucke e Grunes (2017), por exemplo - vêm sendo chamadas de efeitos de rede orientada a dados (*data-driven network effects*), mas, como abordado na Seção 3.1.2.2, essa designação guarda certos inconvenientes, principalmente por tratar como efeitos de rede fenômenos que não são assim caracte-

rizados, a partir de uma abordagem microeconômica. Para evitar ambiguidades, neste trabalho os chamaremos, genericamente, de efeitos de escala, pois em todos os casos é necessário atingir uma massa crítica bastante expressiva, tanto de usuários quanto de volume de dados, para que estes fenômenos sejam efetivamente percebidos.

Todas estas externalidades, que apontam para o mesmo lado, tendem a reforçar posições dominantes e intensificar o acúmulo de dados pessoais, neste último caso, pela articulação das malhas de capilaridade física e lógica, em um processo cada vez mais intensivo provocado pelo *learning by doing*, uma externalidade do lado da produção, também abordada na Seção 3.1.2.2. Adicionalmente, para a melhoria dos sistemas de segmentação, necessita-se de volumes cada vez maiores de dados para a mesma evolução incremental, como discutido na Seção 3.3, o que força as empresas a buscarem novas formas, cada vez mais complexas, ramificadas e eficientes, de acumulação de dados pessoais. Estabelecer a economia da vigilância é, portanto, uma necessidade de negócio.

Com todo esse cenário construído torna-se mais fácil chegar a uma conclusão: os dados pessoais são uma peça importantíssima neste jogo de mercado, mas são apenas uma das peças. Mitigar os riscos aos Direitos Fundamentais e ao livre desenvolvimento da personalidade, potencialmente gerados por estas plataformas, portanto, passa necessariamente por abordar os outros elementos nestas três camadas: arquitetura das soluções, posições ocupadas pelos indivíduos na interação com as plataformas e efeitos de escala.

Inicia-se este capítulo com uma análise da insuficiência e da ineficácia das legislações de proteção de dados pessoais, com enfoque mais atento à GDPR, como garantidoras dos Direitos Fundamentais, em especial a privacidade e o livre desenvolvimento da personalidade. Em seguida, aborda-se a importância da articulação entre os arcabouços normativos pertinentes ao Direito do Consumidor e ao Direito Concorrencial na proteção das liberdades e garantias individuais dos usuários consumidores destas plataformas. Finaliza-se o capítulo com uma sugestão regulatória que propõem a vedação à gratuidade compulsória como forma de mitigar efeitos de escala e aumentar o nível de proteção dos usuários, tanto individual quanto coletivamente.

#### 4.1 *UM PROBLEMA GRANDE DEMAIS PARA AS LEGISLAÇÕES DE PROTEÇÃO DE DADOS PESSOAIS*

Até o final de janeiro de 2020, apenas uma multa havia sido aplicada a uma *Big Tech*, decorrente de violações a previsões legais estabelecidas pela GDPR. A autoridade de proteção de dados francesa, a CNIL, em 21 de janeiro de 2019, multou o Google em 50 milhões de Euros em decorrência de falta de transparência, informação inadequada e falha na obtenção de consentimento válido para personalização de anúncios (CNIL, 2019).

Mais de 20 meses após a entrada em vigor da nova legislação, as autoridades de proteção de dados da Irlanda e de Luxemburgo, países que concentram as sedes das operações europeias das gigantes do Vale do Silício, ainda não apresentaram respostas às denúncias feitas contra essas empresas.

Helen Dixon, que lidera a autoridade irlandesa, em maio de 2019, quando foi ouvida no Senado Americano, e indicou que 51 investigações estavam em andamento contra as *Big Techs* e que as primeiras seriam concluídas ainda no verão de 2019. Até aquele momento, ou seja, menos de um ano da entrada em vigor da GDPR, a autoridade já havia recebido 5.839 reclamações de titulares de dados (em janeiro de 2020 este número já havia subido para 6.716, segundo dados reportados pela autoridade irlandesa à consultoria DLA Piper, para o relatório *GDPR Data Breach Survey* (WECKLER, 2020). Também referiu-se às amplas atribuições da estrutura que coordena (DIXON, 2019):

as autoridades de proteção de dados têm uma gama muito ampla de tarefas, desde promover a conscientização, incentivar códigos de conduta do setor, receber notificações da nomeação de responsáveis pela proteção de dados nas empresas, lidar com reclamações dos consumidores e investigar possíveis violações à GDPR<sup>1</sup>.

A demora para a solucionar reclamações e agir de maneira efetiva para a proteção de dados pessoais envolvendo grandes *players*, em especial os grandes concentradores de dados pessoais que oferecem seus serviços sem contrapartida financeira dos seus usuários, expõe a dificuldade de ação dos órgãos reguladores no combate a condutas potencialmente abusivas realizadas pelos provedores de aplicação. Helen Dixon alega que a GDPR é uma lei ainda não testada e que as decisões tomadas no âmbito da autoridade irlandesa deverão passar pelo escrutínio das autoridades dos 28 países-membros, além de suas cortes nacionais, e que a importância das decisões exige que se leve o tempo necessário para se chegar a conclusões consistentes. Essa situação gera problemas não apenas porque, enquanto não há um posicionamento, potenciais violações a Direitos Fundamentais continuam ocorrendo, mas porque também cria instabilidades entre autoridades e outros órgãos de controle. A situação é resumida, por um membro da autoridade de proteção de dados de Hamburgo, na Alemanha, de modo alarmante (VINOCUR, 2019):

Depois de quase um ano e meio, devemos admitir que temos um enorme problema com a aplicação do tratamento internacional de dados, especialmente por empresas de atuação global. É absolutamente insatisfatório ver que as

<sup>1</sup> Texto original: “data protection authorities have a very broad range of tasks from promoting awareness, to encouraging industry codes of conduct to receiving notifications of the appointment of Data Protection Officers in companies to handling complaints from consumers and investigating potential infringements of the GDPR.” (tradução livre)

maiores violações alegadas de proteção de dados dos últimos 15 meses, com milhões de indivíduos [afetados], estão longe de serem decididas.<sup>2</sup>

Os desafios de garantir a eficácia e o *enforcement*, como nos casos envolvendo a autoridade irlandesa, sobrecarregada com a fiscalização e atendimento às denúncias envolvendo as grandes empresas de internet; o foco excessivo na granularidade do dado pessoal; a centralidade do consentimento, em uma aposta no protagonismo dos indivíduos em gerenciar seus dados pessoais muitas vezes trocados por conteúdos ou serviços em relações que não são claras; um sistema de responsabilização horizontal que se estende a praticamente todas as atividades econômicas nas quais haja participação de seres humanos ao invés de se concentrar esforços nas empresas em que os dados pessoais fazem parte do *core business*. Este é um pequeno resumo dos principais pontos de crítica à GDPR que vêm sendo apontados pela academia<sup>3</sup> e, agora, também, pelas autoridades de proteção de dados<sup>4</sup>, órgãos governamentais dos países europeus<sup>5</sup> e organizações não governamentais<sup>6</sup> e que serão detalhados nesta seção, divididos em duas categorias. A primeira trata-se de uma crítica estrutural, tendo uma obra de Julie Cohen (2019) como ponto de partida. Na segunda, o foco se voltará para fragilidades específicas da legislação, particularmente importantes na regulação do tratamento de dados pessoais realizados pelas plataformas disponibilizadas sem contrapartida financeira do usuário.

#### 4.1.1 Repensar a privacidade e a proteção de dados como um todo?

Em seu artigo *Turning Privacy Inside Out* (COHEN, 2019d), ou Virando a Privacidade do Averso, em uma tradução livre, Julie Cohen sugere que novas bases, tanto teóricas quanto institucionais, sejam lançadas para sustentar o conceito e a proteção da privacidade. Do ponto de vista institucional, inicia a abordagem apontando que a construção discursiva da privacidade, baseada na formulação clássica dos Direitos

<sup>2</sup> No original: "After nearly one and a half years we must concede that we have a huge problem with the enforcement of cross border processing especially by globally acting companies. It is absolutely unsatisfactory to see that the biggest alleged data protection violations of the last 15 months with millions of individuals [concerned] are far away from being sanctioned." (tradução livre)

<sup>3</sup> A título de exemplo, pode-se citar as obras de Koops (2014), Hildebrandt (2015), Purtova(2018), Cohen (2019) e Lynskey (2019).

<sup>4</sup> O caso da autoridade irlandesa, com as dificuldades reportadas para uma ação mais incisivas contra potenciais violações cometidas pelas Big Techs, é um bom exemplo de como a complexidade da legislação está sendo sentida pelas autoridades.

<sup>5</sup> A abordagem da questão dos dados pessoais, no relatório elaborado pela Comissão *Competition Law 4.0*, ligada ao Ministério de Assuntos Econômicos e de Energia da Alemanha, citado na Seção 3.1.2.1 e na Seção 4.2.1.1, é um bom exemplo de como o tema está sendo visto pelos governos, na tentativa de conciliar a necessidade de se manter o fluxo de dados e, ao mesmo tempo, garantir a proteção dos dados pessoais.

<sup>6</sup> Caso do relatório *Competition Policy in a Globalized , Digitalized Economy*, do Fórum Econômico Mundial (2019)



Humanos, traz dificuldades operacionais que, conseqüentemente, tornam a proteção da privacidade "amplamente ineficiente na prática"<sup>7</sup>.

Essa dificuldade, relacionada à proteção da privacidade e, conseqüentemente, dos dados pessoais, devido à forte imbricação destas duas categorias na construção teórica atual, com foco exclusivo nos Direitos Fundamentais, negligenciando que estes últimos também são bens economicamente apreciáveis e em comércio, na prática, já foi abordada na Seção 3.2.1.1, na discussão sobre as contradições entre a GDPR e a Diretiva 2019/770, do Direito Europeu, e os problemas operacionais reais de se compatibilizar uma norma que precisa reconhecer o caráter transacional das relações envolvendo dados pessoais e, ao mesmo tempo, sustentar a indisponibilidade de direitos da personalidade.

A primeira dificuldade prática apontada por Cohen (2019) está, justamente, relacionada ao consentimento, ao afirmar que os sistemas baseados em *notice-and-consent* simplesmente não funcionam. Importante notar, neste ponto, que há uma tendência, que se observa também na abordagem das autoridades de proteção de dados, de reforçar o peso do consentimento como base legal para o tratamento de dados pessoais pelas plataformas e, também, pelos anunciantes, sempre que a atividade esteja relacionada a eficácia ou direcionamento de anúncios, tema absolutamente sensível às plataformas alvos deste trabalho. O posicionamento da autoridade de proteção de dados pessoais do Reino Unido, a ICO, por exemplo, deixa bastante clara essa opção pelo consentimento. No Relatório Atualizado sobre Adtech e leilões em tempo real, ao abordar as bases legais de tratamento, a ICO é clara (ICO, 2019b):

Acreditamos que a natureza do processamento em RTB [em português, Leilão em Tempo Real] torna impossível atender aos requisitos do legítimo interesse como base legal. Isso significa que o legítimo interesse não pode ser usado para o processamento principal da solicitação de lance. Esse seria o caso, mesmo que fosse possível que o legítimo interesse fosse aplicável em outras partes do ecossistema RTB - por exemplo, se uma DMP [em português, Plataforma de Gerenciamento de Dados] for acionada para complementar uma solicitação de oferta com informações adicionais. Parece haver a percepção, por parte de alguns participantes, de que o consentimento é "desafiador" e que o legítimo interesse é a "opção fácil". No geral, não acreditamos que haja um entendimento completo de que exista legítimo interesse. Em nossa opinião, a única base legal para o processamento de dados pessoais por RTB '*business as usual*' é o consentimento (ou seja, o processamento relacionado à colocação e leitura do cookie e à transferência subsequente da solicitação de lance)<sup>8</sup>.

<sup>7</sup> No original: "largely ineffective in practice"

<sup>8</sup> No original: "We believe that the nature of the processing within RTB makes it impossible to meet the legitimate interests lawful basis requirements. This means that legitimate interests cannot be used for the main bid request processing. This is the case even if it were possible for legitimate interests to be applicable elsewhere in the RTB ecosystem – for example if a DMP is asked to supplement a bid request with additional information. There seems to be a perception by some participants that consent is 'challenging' and legitimate interests is the 'easy option'. Overall, we do not believe there is a full understanding of what legitimate interests requires. In our view, the only lawful basis for 'business as usual' RTB processing of personal data is consent (ie processing relating to the placing and reading

Também o Guia de Regras para o Uso de *Cookies* e Tecnologias Similares, emitido pela ICO (2019), segue na mesma trilha. Primeiro esclarece que *cookies* utilizados para fins analíticos, como por exemplo a contagem do número de visitantes únicos, *cookies* relacionados a publicidade, tanto do próprio controlador quanto de terceiros e aqueles usados para conhecer um usuário quanto ele retorna ao *website*, todos direta ou indiretamente ligados à performance de marketing e conversão, não podem ser classificados como estritamente necessários. Depois, conclui que, para todos os *cookies* utilizados para fins diversos daqueles estritamente necessários, a base legal deverá ser, necessariamente, o consentimento.

Neste ponto é importante fazer um registro, para demonstrar como as capilaridades física e lógica, apresentadas na Seção 2.1.2 e na Seção 2.1.3, podem ser articuladas para promover um movimento anticoncorrencial, tema que será tratado na Seção 4.2, e aumentar os riscos a violações de Direitos Fundamentais dos usuários. Em janeiro de 2020, em um anúncio comemorado por muitos, o Google divulgou um plano para banir os *cookies* de seus navegadores Chrome. No comunicado, a empresa vende positivamente a novidade, nos seguintes termos (SCHUH, 2020):

Em agosto [de 2019], anunciamos uma nova iniciativa (conhecida como *Privacy Sandbox*) para desenvolver um conjunto de padrões abertos para aprimorar fundamentalmente a privacidade na web. Nosso objetivo para esta iniciativa de código aberto é tornar a Web mais privada e segura para os usuários, além de dar suporte aos *publishers*. (...) Depois que essas abordagens atenderem às necessidades de usuários, *publishers* e anunciantes, além de desenvolvemos as ferramentas para atenuar os efeitos indesejáveis, planejamos eliminar gradualmente o suporte a *cookies* de terceiros no Chrome. Nossa intenção é fazer isso dentro de dois anos<sup>9</sup>.

As reações foram imediatas. As associações *The Association of National Advertisers* e *American Association of Advertising Agencies*, que representam, respectivamente, anunciantes e agências de publicidade, nos EUA, emitiram uma carta conjunta declarando que “[a] decisão do Google de bloquear *cookies* de terceiros no Chrome pode ter grandes impactos competitivos para negócios digitais, serviços ao consumidor e inovação tecnológica”<sup>10</sup> (SLEFO, 2020).

Considerando a posição dominante do Google no mercado de browser (no mundo, com *market share* de 64%, no Brasil, 82% e nos EUA, 48%, considerando todas as categorias de dispositivos, mas com 61% do mercado em *desktops* (GLOBALSTATS,

of the cookie and the onward transfer of the bid request)”. (tradução livre)

<sup>9</sup> No original: “In August, we announced a new initiative (known as Privacy Sandbox) to develop a set of open standards to fundamentally enhance privacy on the web. Our goal for this open source initiative is to make the web more private and secure for users, while also supporting publishers. (...) Once these approaches have addressed the needs of users, publishers, and advertisers, and we have developed the tools to mitigate workarounds, we plan to phase out support for third-party cookies in Chrome. Our intention is to do this within two years.” (tradução livre)

<sup>10</sup> No original: “Google’s decision to block third-party cookies in Chrome could have major competitive impacts for digital businesses, consumer services and technological innovation” (tradução livre)

2020a) e no mercado de sistemas operacionais para *smartphones*, onde o Android detém 74% do mercado global (GLOBALSTATS, 2020b), este movimento, que só é possível pelo domínio do mercado de navegadores, tanto em computadores quanto em *smartphones*, ou seja, devido às capilaridades lógica e física, coloca o Google na posição de definir e controlar o próximo padrão de fluxo de dados para otimização de publicidade segmentada, um movimento claramente desleal, do ponto de vista da concorrência, pois parte do um ato que não poderia ser praticado por nenhum de seus concorrentes, nem mesmo pelo Facebook. Do ponto de vista do usuário, este movimento reforça a concentração de dados pessoais em um único fornecedor, aumentando ainda mais sua capacidade de segmentação, perfilização e vigilância.

De volta ao artigo, Cohen (2019) reforça toda a complexidade envolvendo os processos de consentimento, que transfere para o indivíduo o ônus de decidir sobre a utilização de seus dados pessoais sem ter, de um lado, informações suficientes para tomar a decisão e, de outro, não possuir o conhecimento necessário para tomar uma decisão com um grau aceitável de segurança, assunto que foi alvo de uma abordagem atenta na Seção 3.1.1. Também debruça-se sobre aspectos importantes relacionados ao aumento da utilização de aplicações baseadas em *machine learning* que, segundo ela, aumentam o nível de vigilância para garantir a efetividade do controle, já que, para esse tipo de solução, as opções do indivíduo quanto à forma de utilização de seus dados devem ser associadas, de alguma forma, aos próprios dados, o que levaria à necessidade de criação de mais uma categoria de dados pessoais: os dados de controle.

Já na construção da teoria da privacidade ao avesso, Cohen aborda a discussão, que ocorre na Europa, sobre a existência de dois direitos fundamentais separados, a privacidade e a proteção dos dados pessoais, em si considerada, com o objetivo de esclarecer como a privacidade poderia ser teoricamente construída não sobre uma formulação baseada no conceito clássico de Direito Fundamental de Liberdade, mas sim com base no conceito de *affordance*:

o direito à privacidade nunca se encaixa particularmente bem nos parâmetros implícitos das formas de discurso mais convencional sobre direitos fundamentais, precisamente porque as expectativas e práticas relacionadas à privacidade são de caráter relacional, contextual e espacial. Uma abordagem baseada em *affordance* para a privacidade promete maior clareza taxonômica. Como ilustração da diferença que essa mudança pode fazer, considere o debate, na doutrina europeia, sobre a proteção de dados ser melhor compreendida como um Direito Fundamental separado ou como uma maneira de implementar certos aspectos do direito fundamental à privacidade. A resposta é: sim - e não. O “direito à privacidade” é uma formulação baseada na liberdade. O “direito à proteção de dados”, que se refere às condições sob as quais os dados pessoais podem ser coletados, processados, usados e retidos, é um direito mais adequado à articulação dentro de um discurso baseado em *affordance*. Esse ponto também ajuda a explicar por que a tendência aparentemente inexorável em direção a notificação e consentimento como condição universal legitimadora para a satisfação das obrigações de proteção

de dados é uma estratégia que está fadada ao fracasso; o consentimento é uma construção baseada na liberdade, mas a proteção eficaz dos dados é, antes de tudo, uma questão de design<sup>11</sup> (COHEN, 2019d).

Cohen não nega a existência de dois direitos separados e defende, inclusive, uma ideia já tratada na Seção 3.2.1.2, de não sobreposição completa entre privacidade e proteção de dados e também de não continência, existindo espaços não cobertos tanto em um quanto em outro. Visto de outra forma, a proteção de dados pessoais age de forma abrangente protegendo não só a privacidade, mas também outros direitos, enquanto, por outro lado, não é suficiente para garantir integralmente a privacidade. A autora reforça, porém, que não apenas a proteção de dados, mas a própria privacidade seja abordada não como um direito de liberdade, mas com base no conceito de *affordance*.

Cunhado pelo psicólogo James J. Gibson (2015), o substantivo *affordance* deriva do verbo *to afford*, que pode ser livremente traduzido, para esse caso, como prover, possibilitar ou disponibilizar, e designa aquilo que um determinado ambiente disponibiliza para quem com ele interage. Representa, portanto, uma situação relacional. Don Norman (2013), por sua vez, adaptou o conceito para o design. Na definição de Norman, *affordance* é uma "relação entre as propriedades de um objeto e as capacidades do agente para determinar quais as possibilidades de uso daquele objeto"<sup>12</sup>. Diferente de Gibson, que falava em *affordances* bons e ruins, Norman trata da existência ou não de *affordances*, dependendo da capacidade do agente em utilizar o objeto. Assim, seguindo o exemplo do próprio autor, toda cadeira possui um apoio em que se permite sentar e muitas cadeiras podem ser transportadas por uma única pessoa (é possível levantar a cadeira), mas algumas só podem ser levantadas por uma pessoa forte ou por várias pessoas. Mas uma pessoa mais fraca pode não ter condições de levantar a cadeira. Para esse caso, a cadeira não tem *affordance* já que o agente não tem a possibilidade de levantá-la. Um outro exemplo ajuda a tornar o conceito mais claro. Uma piscina profunda não tem *affordance* para uma criança de pouca idade, por isso, ao projetar uma piscina infantil, o *designer* deve considerar no projeto a profundidade

<sup>11</sup> No original: "privacy rights have never fit particularly well within the implicit parameters of more conventional forms of discourse about fundamental rights precisely because privacy-related expectations and practices are relational, contextual, and spatial in character. An affordance-based approach to privacy promises greater taxonomic clarity. As one illustration of the difference that such a shift might make, consider the debate among European scholars over whether data protection is best understood as a separate fundamental right or as a way of implementing certain aspects of the fundamental right to privacy. The answer is both — and neither. The "right to privacy" is a liberty-based formulation. The "right to data protection," which is concerned with the conditions under which personal data may be collected, processed, used, and retained, is an entitlement better suited to articulation within an affordance-based discourse. This point also helps to explain why the seemingly inexorable drift toward notice and consent as a universal legitimating condition for satisfaction of data protection obligations is a strategy that cannot hope to succeed; consent is a liberty-based construct, but effective data protection is first and foremost a matter of design." (tradução livre)

<sup>12</sup> No original: "relationship between the properties of an object and the capabilities of the agent that determine just how the object could possibly be used" (tradução livre)

adequada para a faixa etária das crianças que irão utilizá-la. O designer, portanto, tem como objetivo (ou responsabilidade) garantir *affordances* tendo em mira o agente que irá interagir com o objeto.

Portanto, também no design, *affordance* é um conceito relacional, que deve levar em consideração as capacidades e a bagagem cultural do agente. Cohen foi especialmente astuta neste ponto, ao relacionar essa ideia à concretização de Direitos Fundamentais. Ao dizer que, atualmente, cresce o reconhecimento da importância das capacidades de desenvolvimento humano, "abrangendo os recursos necessários não apenas para bem-estar físico, mas também para participação intelectual, cultural e política e autodeterminação"<sup>13</sup> (COHEN, 2019d), e conectar a materialização destas capacidades a um conceito relacional que busca tornar as coisas (aqui tomadas no sentido de objetos, físicos ou não, concebidas por meio do design) mais acessíveis, a autora dá tangibilidade à concretização do Direito. Ao mesmo tempo, transfere responsabilidades de concreção para o designer, mas aceita a existência das limitações inerentes ao próprio objeto. Essa materialização relacional tem uma importância singular quando se discute a eficácia dos Direitos Fundamentais em ambientes quase totalmente mediados por objetos não naturais, ou seja, por objetos, físicos ou digitais, criados pelo homem (*human-made*).

Sob essa ótica, o conceito de privacidade de Hildebrandt (2015), autora que pela primeira vez trouxe à discussão jurídica o conceito de *affordance*, aparentemente mais ligado à ideia original de Gibson do que de Norton, trazido por Cohen (2019), como "o direito de co-determinar como nós seremos lidos"<sup>14</sup> faz bastante sentido, principalmente quando acrescida a ideia, expressa pela própria Hildebrandt (2017) ao comentar criticamente as colocações de Cohen sobre *affordance* e a sua definição de privacidade:

Pode-se dizer que Direitos como Liberdades requerem atenção às capacidades reais de cada pessoa, que por sua vez dependem de *affordances* de seus ambientes institucionais, econômicos e técnicos (que podem ser distinguidos analiticamente, mas não separados na "vida"). Capacidades e *affordances* são, portanto, dois lados da mesma moeda, porque ambos são fundamentados em um entendimento relacional da pessoa humana. São, no entanto, lados diferentes, assumindo a perspectiva do sujeito (capacidades) ou do ambiente (*affordances*). Como não há sujeito sem um ambiente que co-determine suas capacidades e nenhum ambiente sem um agente, levar a sério os Direitos significa levar a sério que o próprio Direito possui recursos específicos que restringem e/ou habilitam as capacidades humanas (que é o principal ponto de Calo). O meu ponto é que essas *affordances* dependem do ICI [em português, Infraestrutura de Informação e Comunicação] onde se fixa a articulação jurídica<sup>15</sup>

<sup>13</sup> No original: "encompass the resources required not only for physical wellbeing but also for intellectual, cultural and political participation and self-determination" (tradução livre)

<sup>14</sup> No original: "the right to co-determine how we will be read" (tradução livre)

<sup>15</sup> No original: "One could say that rights as liberties require keen attention to the actual capabilities of individual persons, which in turn depend on the affordances of their institutional, economic and

A visão de Hildebrandt, portanto, recoloca o Direito como um agente da conformação do ambiente e habilitação das capacidades humanas. Na crítica a Cohen, esclarece que co-determinar como se é lido tem uma abrangência maior do que o direito de não ser lido, pois exige maneiras de levar em conta as modulações do nosso ambiente que, muitas vezes, são realizadas por aplicações baseadas em machine learning “opacas, não testáveis e incontestáveis”<sup>16</sup> e completa afirmando que o sucesso em se efetivar o direito de co-determinar a forma com que se é lido depende da extensão da efetividade de se requerer de atores públicos e privados que sejam disponibilizadas as razões de suas decisões automatizadas (HILDEBRANDT, 2017).

Ainda no seu artigo de respostas aos *reviews* de seu livro, Hildebrandt (2017) cita, em um rodapé, que a Ciência da Computação não pensa em termos de *affordances*. Uma busca na biblioteca virtual do IEEE<sup>17</sup> retorna 798 resultados. Considerando tratar-se de um neologismo relativamente recente, é de se esperar que estes trabalhos acadêmicos tenham alguma relação com as visões de Gibson e/ou Norman. O número de citações ao termo também pode ser considerado elevado o suficiente para, em alguma medida, afastar a ideia de que não há pensamento, na Ciência da Computação, que considere o conceito. Esse comentário ganha relevância quando se relaciona a ideia de interface homem-computador, primeira área onde o conceito foi aplicado na computação, ainda no final dos anos 1980, introduzido pelo próprio Don Norman (STENDAL; THAPA; LANAMAKI, 2016).

O que, talvez, Cohen e Hildebrandt não tenham se atentado é que o próprio Norman fez, no prefácio da edição revisada de seu *The Design of Everyday Things*, onde originalmente apresentou o conceito de *affordance* aplicado ao design, uma ressalva importante sobre as dificuldades de sua aplicação sobre produtos digitais (NORMAN, 2013):

A primeira edição teve foco nas *affordances*, mas apesar das *affordances* fazerem sentido para interações com o mundo físico, elas são confusas quando se lida com objetos virtuais. Como resultado, *affordances* têm criado muita confusão no mundo do design. *Affordances* definem quais ações são possíveis. Significantes especificam como as pessoas descobrem essas possibilidades: significantes são sinais, sinais perceptíveis do que pode ser feito. Significantes possuem importância bem maior para os designers do que *affordances*.<sup>18</sup>

---

technical environment (which can be distinguished analytically but do not lead separate “lives”). Capabilities and affordances are thus two sides of the same coin, because both are grounded in a relational understanding of the human person. They are, nevertheless, different sides, taking the perspective of the subject (capabilities) or the environment (affordances). Since there is no subject without an environment that co-determines its capabilities and no environment without an agent whose environment it is, taking rights seriously means taking seriously that law itself has specific affordances that constrain and/or enable human capabilities (which is Calo’s main point). My point is that these affordances depend on the ICI that roots legal articulation.” (tradução livre)

<sup>16</sup> No original: “opaque, untestable and uncontestable” (tradução livre)

<sup>17</sup> Busca realizada em 31/01/2020 utilizando a URL: <https://ieeexplore.ieee.org/search/searchresult.jsp?newsearch=true&queryText=affordances>

<sup>18</sup> No original: “The first edition had a focus upon affordances, but although affordances make sense

O conceito de *significante*, na forma como formulada por Norman, é uma externalização propositalmente construída, ou seja, é fruto de uma decisão do designer. Os significantes não são relacionais. E esse conceito é particularmente útil onde os ambientes são construídos de forma totalmente artificial como ocorre nos ambientes digitais. Há, de um lado, a explicitação de um ato proposital, mas também a possibilidade de estabelecimento de pontos de controle. Significantes podem ser introduzidos pelos designers e, também, impostos pelo Direito, concretizando, de certa forma, a visão de Hildebrandt.

Visto sob a ótica da eficácia, o mérito da abordagem baseada em *affordances* está em trazer para o Direito não a ideia de inserir aspectos ligados a privacidade e proteção de dados como requisitos de projeto, o que já foi feito com a incorporação do *privacy by design* na nova geração de legislações da qual fazem parte a GDPR e a LGPD, mas de trazer critérios que dão contornos ao bom design. Não se fala, aqui, apenas de requisitos, mas expande-se a abrangência do design como elemento concretizador de direito a partir de critérios de qualidade.

Porém, não há como abarcar todas as circunstâncias envolvendo a proteção de dados pessoais e o exercício do direito à privacidade simplesmente por considerá-los relacionais. O conceito de *affordance*, mesmo na concepção de Gibson, parece não ser abrangente o suficiente. Retomando a preocupação de Hildebrandt sobre a capacidade de se conseguir que atores públicos e privados exponham as razões de suas decisões automatizadas, a articulação da eficácia do Direito para se atingir esse objetivo não passa necessariamente pelo design. O que se observa no ambiente, onde as *affordances* se concretizam, são apenas reflexos de processos computacionais que são executados fora do ambiente e que, muitas vezes, geram reflexos em diversos ambientes paralelos, o que é muito claro nas aplicações de dois ou de múltiplos lados, onde as relações da plataforma com os diversos indivíduos de categorias distintas, mesmo quando realizadas simultaneamente, ocorrem em ambientes também distintos. Portanto, uma resposta satisfatória à preocupação de Hildebrandt não vai emergir do design, nem o conceito de *affordance* poderá ser útil, mas da engenharia poderá surgir resultados satisfatórios.

A ideia de engenharia de privacidade, ou de proteção de dados, também não é nova. Tem correlação direta, atualmente, com engenharia de software, onde seus elementos e categorias são utilizados para projetar sistemas que garantam, ou ao menos maximizem, a proteção de dados. Nesta linha, vale destaque a obra de Michelle Denny, Jonathan Fox e Thomas Finneran (2014). O Direito também pode influir es-

---

for interaction with physical objects, they are confusing when dealing with virtual ones. As a result, affordances have created much confusion in the world of design. Affordances define what actions are possible. Signifiers specify how people discover those possibilities: signifiers are signs, perceptible signals of what can be done. Signifiers are of far more importance to designers than are affordances.” (tradução livre)

tabelecendo critérios de engenharia aplicados a diferentes grupos de tecnologias. Um exemplo prosaico pode dar luz a esta situação. Em abril de 2018, Ben Shneiderman, Cientista da Computação e professor da Universidade de Maryland, uma das principais referências globais da área de interfaces homem-máquina, com contribuições que influenciam diariamente a vida de muitas pessoas como o padrão visual de hiperlinks em páginas web, realizou uma palestra na Universidade de Harvard com o tema *Algorithmic Accountability: Design for Safety*, em que tratava, em uma explicação absolutamente superficial e atécnica, da capacidade dos softwares baseados em *machine learning* de gerarem, em tempo real, informações capazes de possibilitar a verificação das ações tomadas pela aplicação, ou seja, sistemas baseados em machine learning deveriam prover visualizações de seus atos. Ao finalizar a apresentação de Shneiderman, a Profa. Alyssa Goodman, de Harvard, sintetizou a percepção de Ben sobre o assunto, que contém uma aguda carga jurídica: “nós também iremos aprender porque uma importante frase, para Ben, é: ‘*machine learning* sem visualização deveria ser ilegal”<sup>19</sup> (SHNEIDERMAN, 2018).

Uma conclusão é inexorável, em ambientes mediados computacionalmente, a proteção de dados pessoais como garantia e os critérios de disposição dos dados pessoais pelos usuários precisarão ser programados, o que leva a duas outras conclusões: a) serão necessários padrões de design e engenharia, que deverão ser construídos também a partir do Direito e a aplicação destes padrões devem ser fiscalizados pelas autoridades e, em última instância, verificados pelo Direito, tanto no âmbito administrativo quanto judicial, e b) a privacidade, a proteção de dados e o direito do indivíduo de dispor os seus dados passarão a ser entendidos como parte integrante e indissociável do produto.

Apesar de pouco ortodoxa, essa construção teórica pode ser essencial para um aumento de eficácia, por exemplo, da legislação de proteção do consumidor. A qualidade do produto ou serviço é um conceito central das normas de Direito do Consumidor. Trata-se de vocabulário corrente entre consumeristas e categoria conhecida e aplicada pelos tribunais. Neste sentido, à luz do Código de Defesa do Consumidor, tratando do caso brasileiro, é totalmente factível a abordagem de vício de produto ou serviço por falta de garantias de privacidade ou violações à proteção de dados, que vão muito além das vulnerabilidades de segurança da informação e atinam inclusive o tratamento ilegal de dados, por falta de enquadramento nas hipóteses de tratamento previstas na legislação e por inobservância dos direitos dos titulares e dos princípios que devem conformar as atividades de tratamento. No mesmo sentido, torna-se também aplicável a ideia de defeito, atraindo toda a proteção ao consumidor nos casos de fato do produto ou do serviço.

<sup>19</sup> No original: we'll also learn why an important quote from Ben is that machine learning without visualization should be illegal.” (tradução livre)



Parafraseando Hildebrandt (2017), levar os Direitos a sério, no contexto dos ambientes mediados por computador, significa levar a sério o design e a engenharia dos Direitos.

#### 4.1.2 Uma visão crítica sobre a GDPR

As dificuldades de autoridades de proteção de dados pessoais como as apresentadas na abertura deste capítulo, envolvendo a autoridade irlandesa são apenas um exemplo de problemas relacionados à efetividade de legislações extremamente amplas e abrangentes como a GDPR e a LGPD. As avaliações críticas a esta ambiciosa pretensão de controle das atividades de tratamento de dados pessoais vem se acumulando nos últimos anos. Na academia, cada vez mais trabalhos estão sendo escritos<sup>20</sup> apontando problemas estruturais, alguns que podem ser ajustados no próprio contexto da legislação específica e outros que dependerão de complementações vindas de outras áreas, tema que será alvo de tratamento específico na Seção 4.2. Organismos internacionais e governos também começam a fazer conexões entre a privacidade e a proteção de dados (primordialmente reguladas pelas leis gerais sobre o tema, no caso europeu e brasileiro) e outros campos de regulação, como a concorrência. Adicionalmente, a produção legislativa cria novas normas que podem entrar em atrito com as leis de proteção de dados, como demonstrado no caso envolvendo a GDPR e a Diretiva 2019/770, no caso Europeu.

Nesta seção, serão apresentados alguns destes problemas, sempre mantendo o foco nas plataformas digitais utilizadas sem contrapartida financeira e na dificuldade de garantir os Direitos Fundamentais afetados pelo tratamento de dados pessoais. O fio condutor levará em conta o contexto europeu, tendo em vista o histórico de vigência de normas de proteção de dados mesmo anteriores à GDPR, mas sempre que possível será realizado um paralelo com a legislação e o contexto brasileiros.

##### 4.1.2.1 A amplitude dos conceitos de dados pessoais e de tratamento de dados pessoais

O centro gravitacional de legislações de proteção de dados pessoais como a GDPR e a LGPD é a operação de tratamento<sup>21</sup> de dados pessoais. Se não há tratamento, a lei não é aplicável.

No caso brasileiro, por exemplo, a relação entre aplicabilidade e tratamento é explícita, já no art. 3º: “Esta Lei *aplica-se* a qualquer *operação de tratamento*...” - grifo nosso (BRASIL, 2018). Não é diferente no caso europeu, onde a GDPR estabelece,

<sup>20</sup> Apenas a título de exemplo, pode-se citar Cohen (2019), Koops (2014), Lynskey (2019) e Purtova (2018)

<sup>21</sup> Neste trabalho, operação de tratamento e atividade de tratamento são expressões tratadas como sinônimas

no art. 2º, número 1, que “O presente regulamento *aplica-se ao tratamento de dados pessoais...*” - grifo nosso (EUROPA, 2016).

Já o conceito de tratamento, utilizado pelas legislações, pode ser resumido, em uma linguagem coloquial, como qualquer coisa que se faça com um dado. Essa conclusão pode ser extraída, facilmente, das definições do termos previstas nas duas legislações. No caso da LGPD:

art. 5º

(...)

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

Já na GDPR, de onde a previsão da LGPD foi nitidamente inspirada:

Artigo 4.o

(...)

2 “tratamento”, uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

Importante notar que ambas as legislações extrapolam o fluxo de dados, ou seja, até os dados inertes (disponíveis para processamento) são atingidos. Isso demonstra a amplitude extrema do conceito de operação de tratamento. Um limitador desta abrangência poderia ser fixado no alvo das atividades, ou seja, a partir da definição, estabelecida pela legislação, para dados pessoais.

A doutrina identifica duas visões essenciais sobre o conceito de dados pessoais. A visão reducionista exige uma associação direta entre o dado uma pessoa específica. O dado, para ser considerado pessoal, deve ser relacionar a uma pessoa identificada. Já a expansionista não exige uma associação direta entre o dado e uma pessoa natural, mesmo que o vínculo seja indireto, caso a informação possa ser associada a uma pessoa identificável, está-se diante de um dado pessoal (BIONI, 2015).

As legislações, tanto a europeia quanto a brasileira, abarcam o conceito expansionista, ao definirem dados pessoais como toda informação relativa a uma pessoa natural identificada ou identificável<sup>22</sup>. Mesmo considerando esta opção, ainda há uma ampla margem de interpretação quanto à identificabilidade do dado pessoal. Como alertam Schwartz e Solove (2011), a identificabilidade carrega grandes dificuldades de

<sup>22</sup> Artigo 4.o, número 1, da GDPR, e art. 5º, inciso I, da LGPD.

aplicação, tendo em vista que, de um lado, depende do contexto de tratamento e, de outro, se altera com a evolução tecnológica.

Como o caráter contextual se explicita no caso concreto, tanto os órgãos da estrutura de suporte à regulação, como o WP29, no caso da Europa, quanto a própria jurisprudência auxilia na construção mais detalhada da caracterização dos dados pessoais. Nestes processos interpretativos, observa-se que a visão expansionista também está presente.

Ainda em 2007, a WP29 emitiu parecer sobre o conceito de dado pessoal, fazendo uma análise detalhada da expressão central da definição de dados pessoais da Diretiva 95/46/EC, antecessora da GDPR, que se repete na legislação atual e cuja essência também está na definição presente na LGPD: "informação relativa a uma pessoa singular identificada ou identificável"<sup>23</sup>.

Ao tratar da expressão "relativa a", o parecer (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2007) esclarece que um dado diz respeito a (é relativo a) um indivíduo quando está presente um elemento de conteúdo ou um elemento de finalidade ou um elemento de resultado. O elemento de conteúdo significa que trata-se de um dado sobre determinada pessoa natural. Um RFID ou um código de barras associado a um documento de identificação são exemplos trazidos pelo parecer. Já o elemento de finalidade aparece quando os dados são utilizados com o objetivo de "avaliar, tratar de determinada forma ou influenciar" o estado ou o comportamento do indivíduo. O exemplo trazido, para este caso, é a relação de telefonemas realizados por uma pessoa utilizando a infraestrutura de telecomunicações da empresa. A informação pode ser utilizada para diversas finalidades. Sempre que a finalidade envolver uma pessoa natural, este dado será considerado pessoal. Já o elemento de resultado aparece quando o uso da informação pode gerar um impacto provável nos direitos e interesses de uma pessoa. O próprio WP29 esclarece que não é necessário que o resultado tenha grande impacto, basta que a pessoa possa ser tratada de modo diferente a partir da atividade de tratamento. O exemplo trazido é o controle do posicionamento de taxis para otimização dos serviços, gerando impacto nos motoristas.

Na sequência, o parecer aborda a expressão "identificada ou identificável". Ao tratar deste tema, a WP29 explicita o caráter contextual da identificabilidade. Como exemplo, indica que um apelido comum pode não identificar uma pessoa na população de uma cidade, mas certamente identifica um aluno em uma sala de aula específica. No âmbito dos sistemas digitais, geralmente as informações pessoais são aquelas que podem se associar, em alguma circunstância específica, a um identificador da pessoa dentro do sistema, uma chave, na linguagem dos bancos de dados relacionais (ARTICLE 29 DATA PROTECTION WORKING PARTY, 2007). Importante notar que, para

<sup>23</sup> Definição extraída da versão portuguesa da GDPR, por isso a expressão pessoa singular e não pessoa natural como adotado na LGPD. Na versão em inglês: "any information relating to an identified or identifiable natural person" (tradução livre)

a identificabilidade, valem os três elementos de identificação e, existindo apenas um deles, o dado deverá ser considerado pessoal, conseqüentemente haverá operações de tratamento e, naturalmente, a legislação de proteção será aplicável.

Há, neste ponto, uma dificuldade epistêmica. Geralmente, exemplos envolvendo tratamento de dados pessoais são suficientemente simples para serem entendidos. Envolvem um número também relativamente pequeno de categorias de dados, como se observa no parecer da WP29, no caso do exemplo do apelido. Só que esta não é a realidade quando se fala em grandes plataformas digitais globais. O volume de dados e a complexidade das operações muitas vezes tornam a classificação de dados como pessoais irrelevante a priori. O exemplo lapidar, neste caso, são os sistemas de busca ou sistemas de *information retrieval*<sup>24</sup>, em geral. Um dado indexado em um mecanismo de busca é um dado pessoal? Como se pode concluir, a partir das explicações dadas pelo WP29, não há uma resposta imediata e apriorística a esta pergunta. Há dados pessoais indexados nos sistemas de busca? Certamente há. Dessas incerteza geral e certeza específica nascem outras perguntas. Do volume total de dados tratado, quanto representaria os dados pessoais? Seria possível fazer restrições específicas ao tratamento desses dados? Há viabilidade de estabelecer critérios de tratamento, numa operação de busca, onde a identificação de determinada informação como pessoal pudesse fazer diferença?

O famoso caso *González v. Google* pode servir de base para algumas conclusões relevantes. Nele, Mario Costeja González, apresentou uma reclamação à Agência Española de Protección de Datos (AEPD) solicitando a retirada, dos resultados de busca do Google, do link para duas páginas do jornal *La Vanguardia* que continham um anúncio de venda de imóveis, em hasta pública, decorrente de arresto para pagamento de dívidas com a Seguridade Social, em que o nome M. Corteya González era mencionado. A AEPD acatou o pedido e determinou a retirada dos resultados, decisão que foi contestada judicialmente pelo Google. Em decisão final, o Tribunal de Justiça da União Europeia ratificou a posição da AEPD, ordenando a supressão dos resultados e declarando, especificamente sobre tratamento de dados pessoais, ainda sob a égide da Diretiva 95/46/CE:

O artigo 2.o, alíneas b) e d), da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, deve ser interpretado no sentido de que, por um lado, a atividade de um motor de busca que consiste em encontrar informações publicadas ou inseridas na Internet por terceiros, indexá-las automaticamente, armazená-las temporariamente e, por último, pô-las à disposição dos internautas por determinada ordem de preferência deve ser qualificada de "tratamento de dados pessoais", na aceção do artigo 2.o, alínea b), quando essas infor-

<sup>24</sup> *Information retrieval*, ou recuperação de informações, é a designação geral para sistemas desenvolvidos para recuperar informações extraídas de documentos, geralmente envolvendo grandes volumes de dados

mações contenham dados pessoais, e de que, por outro, o operador desse motor de busca deve ser considerado "responsável" pelo dito tratamento, na aceção do referido artigo 2.º, alínea d).

Difícil enxergar claramente, a partir da declaração, a que operação ou atividade a expressão "tratamento de dados pessoais" se refere neste contexto. Não parece razoável entender a expressão relacionada ao fornecimento do serviço de busca como um todo. Pode-se enxergar atividade de tratamento na própria indexação, ou seja, no processo de criação dos índices e reestruturação do conteúdo para permitir a rápida recuperação das informações. Mas uma imposição como esta criaria uma dificuldade operacional imensa, primeiro por criar um procedimento classificatório prévio que, além de extremamente difícil, poderia carregar vieses relevantes gerados pela própria atividade de classificação. Além disso, implementar um sistema classificatório interferiria no modo de arranjo das informações, certamente com impactos na performance dos serviços, já que os dados são organizados com o objetivo específico de serem rapidamente recuperados e apresentados ao usuário. Na ausência de pré-classificações, não há classificação prévia de dados pessoais, ou seja, a declaração exarada pelo Tribunal só será eficaz, na prática, mediante a reclamação do indivíduo que sentiu sua esfera de direitos atingida. Não há eficácia preventiva. Neste sentido, as conclusões de Schwartz e Solove (2011) sobre o caso, mesmo sendo feitas antes da decisão final do Tribunal de Justiça da União Europeia continuam válidas:

a questão de saber se as consultas de pesquisa são dados pessoais<sup>25</sup> não pode ser respondida em abstrato. É inútil tentar classificar as consultas de pesquisa como dados pessoais ou dados não pessoais para ajustá-las ao sistema binário de muitas regulamentações de privacidade atuais. As consequências das consultas de pesquisa dependerão do contexto, como as coisas específicas pesquisadas, bem como de quais outras informações já estão disponíveis sobre um usuário<sup>26</sup>.

O caso dos buscadores dá uma pista interessante sobre a eficácia da proteção dos Direitos Fundamentais em plataformas digitais. O deslocamento das medidas protetivas dos direitos da personalidade da atividade de tratamento para o resultado efetivo. Este deslocamento, no caso das grandes plataformas, ainda tem uma outra vantagem que não é evidente no caso *Gonzales vs. Google*. No caso espanhol, é fácil identificar o dado pessoal gerador da violação ao direito individual. Assim, mesmo que só seja possível identificar os dados pessoais que causaram a violação depois

<sup>25</sup> A Associação Brasileira de Normas Técnicas (ABNT), na tradução da norma ISO/IEC 27701 traduziu "personally identifiable information" (PII) como dado pessoal justificando a escolha pelo uso corrente da expressão no Brasil. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2019)

<sup>26</sup> No original: "the question of whether search queries are PII cannot be answered in the abstract. Trying to classify search queries as PII or non-PII in order to fit them into the binary system of much current privacy regulation is futile. The consequences of search queries will depend upon the context, such as the specific things searched for, as well as what other information is already available about a user." (tradução livre)

de tê-la constatado, sendo praticamente impossível evitá-la a priori, pode-se agir para suprimir ou restringir suficientemente as atividades de tratamento sobre esses dados para que se cesse a violação aos direitos do indivíduo. Mas em muitos casos, não é possível fazer essa distinção. Nos complexos sistemas de leilão de publicidade, que sustentam as plataformas digitais pretensamente gratuitas, quais dados pessoais são utilizados para segmentar o anúncio apresentado para o usuário? Mesmo que o usuário desabilite os anúncios segmentados, o próprio contexto da aplicação, por exemplo, os termos de busca ou o conjunto de informações que aparecem na *timeline*, que não são diretamente do usuário, mas que carregam conteúdo suficiente, além dos perfis de quem efetivamente postou aquelas informações, já não geram informações suficientes para segmentação de anúncios? Essas são perguntas difíceis de serem respondidas. Mais do que isso, a complexidade das plataformas torna muito difícil os processos de fiscalização, principalmente se for levado em conta a atomização das atividades de tratamento. Atuações regulatórias sobre o resultado, sempre que possível, podem ser boas alternativas para as incertezas e os riscos envolvidos em processos complexos de tratamento de dados pessoais.

O fato observado no caso dos mecanismos de busca não permite concluir que a classificação de determinada informação como dado pessoal seja genericamente inútil ou que não deva ser feita. Pelo contrário, a classificação e as preocupações com as atividades de tratamento continuam sendo relevantes, principalmente quando o foco é direcionado para os dados estruturados (aqueles armazenados em bancos de dados relacionais, por exemplo), mas não se mostra eficiente quando há tratamento de dados não estruturados ou semi-estruturados. Nestes casos, a translação do centro de gravidade, saindo da operação de tratamento e se deslocando para o resultado final pode ser uma alternativa para aumento do nível de eficácia. Muitas soluções baseadas em *machine learning*, por exemplo, processam dados não estruturados ou semi-estruturados e as próprias características destes sistemas tendem a dificultar a identificação das operações efetivamente realizadas para se obter determinado resultado. Por este motivo, mantendo o foco no resultado, a atuação regulatória passará, inevitavelmente, pelo estabelecimento de critérios de design e engenharia, como apresentado na Seção 4.1.1. Somente desta forma será possível intervir no resultado, a priori, para garantir maior proteção aos Direitos Fundamentais, ou apurar responsabilidade, caso ocorra uma violação de direito geradora de dano. Um exemplo para esta última situação seria o estabelecimento da obrigatoriedade de *algorithmic accountability* para aplicações baseadas em *machine learning* também apresentada na Seção 4.1.1.

Interpretações muito expansionistas também podem gerar uma situação onde praticamente qualquer informação pode ser, em alguma circunstância, classificada como dado pessoal. Nadezhda Purtova (2018) publicou um interessante artigo nome-

ando a GDPR como a lei aplicável a tudo (“the law of everything”) e alertando para os riscos de uma legislação que “entrega uma alta proteção legal para todas as circunstâncias, mas que na prática é impossível de cumprir sendo, portanto, ignorada ou desacreditada, levando ao abuso de direito e à irracionalidade”<sup>27</sup>. No artigo, a autora traz um exemplo interessante apontando que, dependendo das circunstâncias de tratamento de dados, até mesmo as informações sobre as condições climáticas poderão ser classificadas como dados pessoais, caso sejam utilizadas em associação com outros dados que permitam a identificação de um indivíduo para uma finalidade específica. Neste caso, o elemento de identificação, tendo como referencial o parecer da WP29 (2007) é a finalidade.

Mesmo quando aborda o elemento de conteúdo, ou seja, quando se trata de um dado sobre uma pessoa, o enquadramento pode não ser claro e exigir uma interpretação, que pode ser expansionista ou reducionista. No Brasil há um caso que, dependendo da interpretação a ser pacificada, seja pela Autoridade Nacional de Proteção de Dados (ANPD) ou pela jurisprudência, poderá gerar um aumento não desprezível nos custos de compliance e adequação à LGPD. As informações de um Microempreendedor Individual (MEI) devem ser consideradas dados pessoais? Para contextualizar, o art. 18-A, § 1º, da Lei Complementar 123, estabelece que a natureza jurídica do MEI é empresário individual. Já o Cadastro Nacional de Atividade Econômica (CNAE) descreve o seguinte (INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA, 2018):

213-5 - Empresário (Individual)

o empresário pessoa física que exerce profissionalmente atividade econômica, organizada para a produção ou circulação de bens ou de serviços, sem se constituir pessoa jurídica e sem a participação de qualquer sócio, mas que, para fins do Imposto de Renda é equiparado à pessoa jurídica. É obrigatória a inscrição do empresário na Junta Comercial, antes do início de sua atividade. O empresário responde ilimitadamente pelas obrigações empresárias assumidas. Base legal: Código Civil (Lei 10.406 de 10/01/2002, art. 966 e seguintes)

Em uma visão expansionista a resposta é sim, já que trata-se da pessoa natural que cumpre uma exigência fiscal inscrever-se no Cadastro Nacional de Pessoa Jurídica (CNPJ) para executar uma atividade empresária. Neste caso, informações relacionadas a um CNPJ passariam a ser consideradas dados pessoais. Já na visão reducionista chega-se à conclusão oposta. Os dados de um MEI não podem ser considerados pessoais, pois equipara-se a uma pessoa jurídica para fins do Imposto de Renda, necessitando inclusive de registro na Junta Comercial. Na prática, também age, em todas as suas relações jurídicas com terceiros, como se pessoa jurídica fosse. A opção

<sup>27</sup> No original: “deliver the highest legal protection under all circumstances, but in practice impossible to comply with and hence ignored or discredited as conducive to abuse of rights and unreasonable” (tradução livre)

reducionista, por sua vez, dissocia definitivamente os conceitos de pessoa física e pessoa natural, já que algumas informações do acervo de dados da primeira não fariam parte do acervo da segunda.

O impacto dessa decisão na gestão de conformidade à LGPD é imenso. Significa extrapolar, para os dados gerados a partir do relacionamento com as pessoas jurídicas, todas as ferramentas e procedimento de controle e de gestão de direitos a titulares de dados pessoais para atender a uma exceção, representada pelo MEI, uma pessoa física revestida por uma armadura de pessoa jurídica.

Purtova (2018) sugere, como forma de minimizar este problema, “abandonar o conceito de dados pessoais como pedra angular da proteção de dados e buscar soluções para os ‘danos informacionalmente induzidos’ [*information-induced harms*] - entendidos amplamente como qualquer consequência negativa, individual ou pública, decorrente de processamento de informações”<sup>28</sup>. A sugestão de Purtova encontra dificuldades evidentes. Primeiro porque parte da premissa de que se deve aceitar que todos os dados são pessoais, posição ratificada pela autora na sua conclusão, o que definitivamente não é verdade. Mesmo com essa posição radical, a sugestão também possui caráter ampliativo porque sugere que análises de impacto sejam extrapoladas para todas as situações, o que simplesmente transferirá a carga de conformidade do mapeamento de dados e da identificação das atividades de tratamento para uma nova categoria que concentra diversas atividades de tratamento não mais restritas ao dados pessoais, mas a qualquer conjunto de dados.

Há, porém, um mérito importante no trabalho de Purtova, ligado ao fato de que é necessário se fixar atenção ao resultado, ao que denominou de *information-induced harms*. Mas o ponto focal não sai da classificação (ou não) dos dados pessoais. Este deslocamento acontece pela transferência da centralidade da operação de tratamento para o resultado. Além disso, mesmo com a mudança de foco, os padrões de atuação para proteção efetiva dos Direitos Fundamentais também precisam ser ampliados para extrapolar as análises e avaliações de risco, chegando até à definição de padrões técnicos capazes de aumentar o nível de proteção, em uma abordagem de Direito como design e engenharia.

Como abordado anteriormente, esta deve ser uma abordagem complementar, tendo em vista que para os casos que envolvem, essencialmente, dados estruturados os métodos de controle focados na operação de tratamento podem funcionar adequadamente. Isso significa que, na prática, o problema da ampliação da abrangência do conceito de dados pessoais, que provoca a incidência da legislação de proteção aplicável a tudo ainda persiste.

Koops (2014) também apresenta uma solução radical para este problema, su-

<sup>28</sup> No original: “to abandon the concept of personal data as a cornerstone of data protection altogether, and seek remedies for ‘information-induced harms’ – understood broadly as any individual or public negative consequences of information processing” (tradução livre)



gerindo o fim das legislações gerais, com aplicabilidade ultra extensiva, muito devido à grande amplitude do enquadramento das informações como dados pessoais. Sugere a criação de regimes *sui generis* de regulação por tipos de dados ou tipos de problemas a serem enfrentados. Também neste caso, aponta-se para os efeitos (resultados) do processamento de dados e não para a existência de dados pessoais ou a identificação e controle das atividades de tratamento atômicamente consideradas. Também indica que para determinados casos, ao invés de regulações *sui generis*, dispostas de modo esparso, as questões ligadas a tratamento de dados pessoais podem ser tratadas por leis específicas já existentes:

Alguns problemas também se assemelham aos problemas tratados em outros campos e a proteção de dados também pode ser alcançada tornando o processamento justo de dados parte integrante desses campos. A portabilidade de dados, por exemplo, poderia muito bem ser regulada pela lei de proteção ao consumidor, enquanto o uso de identificadores on-line pode ser regulamentado (e até certo ponto é regulamentado, embora não particularmente bem) no comércio eletrônico, telecomunicações e mídia<sup>29</sup>

Vale lembrar que leis gerais não são uma unanimidade. A recente legislação da Flórida, sobre dados pessoais, a California Consumer Privacy Act (CCPA), restringe-se ao tratamento de dados pessoais no escopo das relações de consumo. Trata-se de uma alternativa coerente, mas uma proteção mais específica para determinados tipos de relação ou de categorias de dados não precisa, necessariamente, prescindir de uma lei regente. É possível se pensar em regulações específicas que reforcem o nível de proteção aos Direitos Fundamentais ligados ao tratamento de dados pessoais dentro de um regime geral que, por exemplo, incluam regras de limitação de abrangência.

A própria GDPR, no sentido de limitar obrigações, já adota esse procedimento. No artigo 35, por exemplo, impõe a necessidade de avaliação de impacto das operações de tratamento para atividades que impliquem em “elevado risco para os direitos e liberdades das pessoas singulares”. Já o artigo 30 isenta a obrigatoriedade de registro das atividades de tratamento para empresas com menos de 250 trabalhadores, que não realizem atividades de tratamento suscetíveis “de implicar um risco direto para os direitos e liberdades do titular dos dados” e que tais operações sejam ocasionais e não envolvam dados pessoais sensíveis. O artigo 37, por sua vez, restringe a necessidade de nomeação de Data Protection Officer (DPO) - encarregado, na dicção em português, da GDPR. Considerando organizações privadas, há necessidade de nomeação sempre que a atividade principal do responsável (controlador) ou do subcontratante (operador) consista em operações de tratamento que, “devido à sua natureza, âmbito

<sup>29</sup> No original: “Some problems also resemble problems dealt with in other fields, and data protection can also be achieved by making fair data processing part and parcel of those fields. Data portability, for example, could well be regulated in consumer protection law, while the use of online identifiers can be regulated (and to some extent is regulated, although not particularly well) in electronic commerce, telecommunications, and media law.” (tradução livre)

e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala” ou envolvam tratamento em grande escala de dados sensíveis ou de condenações penais e infrações (EUROPA, 2016).

A LGPD, a seu turno, traz previsões similares e conta com um nível de abertura maior, tendo em vista que muitas modulações de abrangência foram atribuídas à ANPD. Especificamente quanto ao porte e a tipos específicos de atividades, o art. 55-J, inciso XVIII prevê como atribuição da autoridade “editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de carácter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se” à lei (BRASIL, 2018).

Seria possível, também, adotar uma solução similar à proposta por Schwartz e Solove (2011), de dados pessoais 2.0, baseado no risco de identificação, em um espectro que vai dos dados sem nenhum risco de identificação até dados que identificam univocamente uma pessoa. De todo modo, como amplamente exposto nesta seção, em casos envolvendo dados não estruturados ou semi-estruturados, a classificação a priori é pouco útil e a adoção de um espectro de classificação baseado nas características do dado em si não diminui, necessariamente, a amplitude de aplicação da legislação.

Mais uma vez, considerar os efeitos ou resultados, parece ser mais indicado para limitações de abrangência. É importante notar que estes critérios já são utilizados pela GDPR, por exemplo, para limitações de obrigação. Levar em consideração o “elevado risco para os direitos e liberdades das pessoas singulares” (EUROPA, 2016) refere-se diretamente os efeitos e não às atividades de tratamento em si. Criar hipóteses mais amplas de isenção das obrigações estabelecidas na legislação geral, aplicáveis a, por exemplo, atividades de baixo risco, pode ser uma alternativa viável para barrar o expansionismo da incidência das leis de proteção de dados pessoais. Uma crítica legítima a este modelo seria o elevado grau de subjetividade no enquadramento de uma operação como de baixo risco. A resposta mais direta está no fato de que já há, na legislação atual, um parâmetro cujo enquadramento exige o mesmo grau de subjetividade, em um extremo até mais perigoso, como é o caso das atividades que envolvem alto risco aos direitos e liberdades.

A questão da amplitude do conceito de dados pessoais, portanto, deve ser encarada como um mecanismo de dosagem dos esforços de controle, permitindo a flexibilidade suficiente que viabilize o aumento da proteção aos Direitos Fundamentais, concentrando mais proteção aos dados pessoais em circunstâncias que envolvem maiores riscos e eliminando (ou diminuindo drasticamente) as obrigações de controle em atividades de tratamento que gram pouco risco. Esse novo balanceamento, aliado a regulações complementares em outros campos, como o Direito do Consumidor

e o Direito Concorrencial, tendem a aumentar a eficácia de proteção e diminuir a probabilidade de colapsos como os profetizados, com razão, por diversos autores.

#### 4.1.2.2 Como identificar o responsável, se a responsabilidade é de todo mundo?

Em julho de 2019, o Tribunal de Justiça da União Europeia decidiu que a Fashion ID, uma plataforma de e-commerce de moda, com sede na Alemanha, deveria ser considerada controladora, juntamente com o Facebook, pela simples disponibilização do botão de *like* nas páginas dos produtos à venda. Ao final de um longo Acórdão, o Tribunal apresenta quatro declarações, com algumas conclusões bastante relevantes sobre os critérios utilizados para a definição de controladores (responsáveis, na dicção portuguesa), o escopo da atividade de coleta de dados e limitações de responsabilidade.

Na declaração de número dois, o Tribunal de Justiça da União Europeia deixa claro que o núcleo interpretativo das legislações de proteção de dados é a operação de tratamento. Também delimita, mais claramente, o significado de coleta (recolha ou *collection*, em inglês) como uma operação de criação de oportunidade para que um dado seja processado por alguém, não necessariamente por quem realizou a operação de coleta. Na disponibilização do botão de *like*, a Fashion ID não realiza o processamento dos dados, mas simplesmente cria uma oportunidade para que o Facebook realize esse processamento. A decisão, no seu parágrafo 69, deixa essa situação muito clara, ao afirmar que “a responsabilidade conjunta de vários intervenientes pelo mesmo tratamento, por força desta disposição [definição de controlador, na alínea d, do art. 2º, da Diretiva 95/46/CE], não pressupõe que cada um deles tenha acesso aos dados pessoais em causa” (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2019). Ainda na mesma declaração, o Tribunal ressalta a limitação da responsabilidade do controlador às atividades por estes efetivamente realizadas.

Outro ponto relevante da decisão refere-se ao peso dado pelo tribunal ao aproveitamento econômico como critério de definição do controlador. A inclusão do botão de *like*, pela FashionID, tem como objetivo otimizar a publicidade de seus produtos na plataforma de rede social (Facebook) e, com o objetivo de obter esta vantagem, a FashionID cria as condições para que os dados sejam colhidos e transmitidos. Fica, evidente, portanto, a existência de uma vantagem econômica tanto para a FashionID quanto para o Facebook, tornando inevitável, sob esta ótica, o enquadramento das duas empresas como controladores conjuntos. O parágrafo 80 do acórdão deixa claro a utilização deste critério (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2019).

A declaração de número três aborda o legítimo interesse. Esclarece que, se no caso for aplicável o legítimo interesse, deve-se levar em consideração os legítimos interesses de ambos os controladores, considerando as operações de tratamento executadas por cada um deles. Importante notar que o Tribunal não convalida o legítimo

interesse como base legal para esse tipo de tratamento, mesmo porque reconhece que, havendo a utilização de *cookies*, a regulamentação nacional da Diretiva 2002/58 pode exigir explicitamente o consentimento prévio para seu armazenamento nos dispositivos dos usuários, o que inviabilizaria o legítimo interesse como hipótese de tratamento (parágrafo 89). Já no parágrafo 91, justifica a necessidade de abordagem do legítimo interesse por não se poder garantir que os dados pessoais tratados restringiam-se a informações processadas a partir da utilização de *cookies* (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2019).

Já a declaração de número quatro trata do consentimento, essencial, no caso concreto, para o tratamento de dados pessoais obtidos a partir de *cookies*. Neste ponto, importante observar que, além das regulações locais da Diretiva 2002/58, começa-se a formar um entendimento sólido quanto à necessidade de consentimento para operações envolvendo *cookies* e tecnologias correlatas também no âmbito das autoridades nacionais de proteção de dados. O *Update Report sobre Adtechs e Leilões em Tempo Real* (ICO, 2019b) e o Guia sobre Uso de *Cookies* e Tecnologias Similares (ICO, 2019a), ambos da ICO, expressam este posicionamento. Além disso, a quarta declaração reforça o dever de informação (nas legislações atuais, derivado do princípio da transparência) ao usuário, titular dos dados pessoais alvo do tratamento, sobre as operações que envolvem a disponibilização do botão, nos limites daquelas realizadas pelo responsável pelo site (TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, 2019).

Merecem atenção, neste caso, alguns comentários expressos nas Conclusões do Advogado-Geral, Michal Bobek (2019), sobre os impactos de longo prazo desta decisão, começando pela pergunta expressa no parágrafo 71: “A proteção efetiva pode ser reforçada se todos forem responsáveis por garanti-la?”. Depois de um longo percurso, conclui:

92. Além disso, em resposta à questão colocada no início desta secção (n.º 71), uma pessoa cética originária das partes mais orientais da União Europeia pode talvez sugerir, considerando a sua experiência histórica, que a proteção efetiva de algo tende a diminuir drasticamente se todos foram responsabilizados pela mesma. Tornar todos responsáveis significa que ninguém será de facto responsável. Ou melhor, é provável que a única parte que deveria ter sido considerada responsável por uma determinada ação, aquela que exerce efetivamente controlo, se esconda atrás de todos os outros designados “corresponsáveis”, sendo a proteção efetiva provavelmente diluída de forma significativa.

A conclusão do Advogado Geral é precisa. Se, por um lado, a decisão de considerar controlador aquele que administra site ou aplicação que utiliza partes de terceiros cria uma barreira de consentimento que, em tese, permite barrar a capilaridade lógica de grandes plataformas, como ocorre no caso de Fashion ID e Facebook, por outro, cria um monstruoso desafio fiscalizatório, pois transfere a responsabilidade para milhões de organizações que utilizam este tipo de conector social que poderão, ou não,

seguir a orientação estabelecida pelo Tribunal, juntamente com as determinações das autoridades nacionais. Também cria uma zona de conforto para a plataforma, pois todas as responsabilidades relativas às operações de coleta e transmissão passam a ser daquele que incluiu o código na página, isentando, em grande medida a própria plataforma por integrações realizadas em desconformidade com a legislação de proteção de dados pessoais. Por fim, também transfere parte do ônus para o próprio usuário, titular dos dados pessoais, que terá que executar as avaliações de consentimento para cada um dos sites que contenham esse tipo de conteúdo, enfrentando todas as dificuldades inerentes às decisões desta natureza, já detalhadas na Seção 3.1.1 deste trabalho.

Isso não significa que a questão dos botões de *like*, caso claro de expansão de capilaridade lógica, não seja relevante do ponto de vista da proteção aos Direitos Fundamentais dos usuários. Pelo contrário, trata-se de um recurso bastante eficiente para fins de perfilização, pois a disponibilização do botão permite que dados do usuário sejam coletados mesmo que eles não cliquem no botão. Em certo sentido, o *like* é um botão de rastreie-me. O que se coloca, como contraponto da decisão do Tribunal de Justiça da União Europeia, é a questão da eficácia de longo prazo. Uma solução que pulveriza responsabilidade pode dar, inicialmente, uma sensação de maior controle que, na verdade, é falsa, podendo inibir, inclusive, a busca por soluções mais eficazes, centradas nas grandes plataformas que baseiam seus negócios no tratamento massivo de dados pessoais.

#### 4.1.2.3 Foco no *compliance* e não na proteção de dados pessoais

Tanto a GDPR quanto a LGPD definem *accountability* como um princípio a ser seguido nas atividades de tratamento de dados pessoais. O art. 5.o, n.o 2, da GDPR possui a seguinte dicção: “O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo (“responsabilidade”)”. No texto em inglês, o equivalente à palavra responsabilidade, no texto legal, é *accountability*. A LGPD apoiou-se na amplitude, mas não cedeu ao anglicismo na redação do inciso X, do art. 6º, que fixa como princípio a responsabilização e a prestação de contas, exigindo a “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. É necessário, portanto, agir em conformidade (*compliance*) e demonstrar que se age em conformidade.

Na Seção 2.2.2, ao abordar o modo como as empresas de tecnologia moldam a regulação do setor, o “empreendedorismo legal-institucional”, na expressão cunhada por Cohen (2019), busca formas de autorregulação, muitas vezes tornadas efetivas a partir da atuação de entidades não estatais, com ou sem fins lucrativos, no processo de regulação (COHEN, 2019a). Em outra tática de modelagem, parte das atividades

de fiscalização passam a ser terceirizadas para a própria organização fiscalizada, em um processo colaborativo e co-regulatório realizados em padrões de consenso, que orientam o *compliance* e o *enforcement*, geralmente definidos pelas entidades não estatais de apoio (COHEN, 2016).

Ao modelo regulatório co-participativo, que pode ser engendrado para enfraquecer as estruturas fiscalizatórias, acresce-se um outro problema, também bastante grave, ligado à prestação de contas. Legislações como a GDPR e a LGPD estabelecem não apenas obrigações negativas, de limitação das operações de tratamento de dados com vista à proteção dos direitos dos titulares, mas também define uma série de obrigações positivas de demonstração de conformidade bastante horizontais, aplicáveis a praticamente todas as organizações que fazem tratamento de dados pessoais. Como o pacto de co-regulação delega atividades de controle para o agente de tratamento, resta aos órgãos estatais avaliar a conformidade por meio das evidências documentadas pela organização fiscalizada. Assim, não é difícil que a atenção dos responsáveis pela conformidade às legislações de proteção de dados, nas organizações, desloquem seus pontos focais da proteção de dados em si e passem a fixar atenção e esforços na geração de elementos que comprovem a conformidade. As organizações passam, então, a investir recursos na prestação de contas. Com o investimento, nasce um novo mercado com sua lógica própria. Neste sentido, são precisas as colocações de Purtova (2018):

Diante da ameaça de sanções efetivas e dissuasivas, os controladores, em vez de se envolverem em uma avaliação significativa de lealdade e necessidade, são pressionados a criar a aparência formal de conformidade usando “substitutos de conformidade”, como roteiros de conformidade, “ferramentas de *accountability*”, *trust marks* e sistemas de certificação. O último provavelmente será fornecido por entidades privadas - escritórios de advocacia, consultorias e empresas de auditoria - que atuam no negócio de venda de confiabilidade mais do que salvaguardam os interesses de proteção de dados e cujos produtos são comprados para validar e comunicar *compliance* aos acionistas, titulares de dados e autoridades de proteção de dados<sup>30</sup>.

Esse sistema baseado em um mercado da conformidade pode, muitas vezes, criar mecanismos que trabalham na linha limite entre o atendimento à legislação e a violação aos direitos e garantias dos titulares. O pensamento passa a ser o de viabilização das operações de tratamento, com o menor impacto operacional possível dentro de níveis de risco aceitáveis, deixando claro que a proteção efetiva dos dados pessoais possui importância secundária.

<sup>30</sup> No original: “Facing the threat of effective and deterring sanctions, the controllers, instead of engaging in a meaningful assessment of fairness and necessity, will be pushed to create the formal appearance of compliance by using ‘compliance surrogates’, such as compliance roadmaps, ‘accountability tools,’ trust marks and certification schemes. The latter will likely be provided by private entities – law firms, consultancies and audit firms – who are in the business of selling reassurances more than safeguarding data protection interests, and whose products are bought to validate and broadcast compliance to the shareholders, data subjects and the data protection authorities.” (tradução livre)

Em sistemas complexos como as plataformas digitais, todo o arcabouço de demonstração de conformidade tende a ser imenso, exigindo esforços consideráveis para análise pelos órgãos de controle. Muitas vezes, o excesso cria embaraços que ajudam a retardar os processos fiscalizatórios e a consumir os recursos das autoridades de proteção de dados que, além dos casos complexos que envolvem riscos reais aos Direitos Fundamentais dos titulares de dados, precisa ser capaz de dar vazão a grandes volumes de denúncias relativas a casos onde, mesmo havendo algum tipo de inconformidade com a legislação, não há riscos reais consideráveis aos direitos dos titulares.

#### 4.2 DIREITO DO CONSUMIDOR E CONCORRENCIAL NA DEFESA DOS DIREITOS FUNDAMENTAIS

Na décima edição do Seminário de Proteção à Privacidade e aos Dados Pessoais, organizada pelo Núcleo de Informação e Coordenação do Ponto BR (nic.br) e pelo Comitê Gestor da Internet no Brasil (cgi.br), a Conferência de Abertura ficou a cargo de Orla Lynskey (2019), *Associate Professor* na *London School of Economics*. Com o sugestivo título *Proteção de Dados Através do Espelho*<sup>31</sup>. O título, que remete ao mundo invertido de Lewis Carroll, sugere o objetivo de Lynskey, de repensar as bases que fundamentam a proteção de dados e virá-la de ponta cabeça. Para isso, parte da necessidade de mudanças em duas frentes, na regulação da proteção de dados pessoais. A primeira, interna, nas legislações específicas de proteção de dados, aliando, ao amplo conjunto de direitos e responsabilidades, novos mecanismos que tornem o *compliance* e o *enforcement* mais eficazes, já que olhando para a experiência europeia de proteção de dados, “enquanto a lei, no papel, é muito sólida, na prática tem sido muito ineficaz”<sup>32</sup>. A segunda, externa, exige ir além da regulação da proteção de dados, avançando para outras áreas do Direito, como o Direito do Consumidor e, principalmente para o Direito Concorrencial com foco nas empresas que possuem posição dominante no mercado.

A correlação de privacidade e proteção de dados com mecanismos antitruste tem ganhado evidência, na medida em que se percebe os movimentos das companhias no sentido de reforçarem as externalidades positivas, tanto os efeitos de rede quanto o “learning by doing”, fenômenos tratados em maiores detalhes na Seção 3.1.2.2. Também fica cada vez mais claro que, para as plataformas que possuem a disponibilização de oportunidades de publicidade para anunciantes, a concentração da remuneração financeira do lado inverso ao usuário viabiliza um crescimento de faturamento em uma escala superior à linear, como acontece nos casos de Facebook e Tencent onde o cres-

<sup>31</sup> Data Protection Through the Looking Glass (tradução livre)

<sup>32</sup> No original: “while the law on the books is very solid the in practice has been very ineffective.” (tradução livre)

cimento é quadrático em relação ao número de usuários, como indicam os trabalhos de Metcalfe (2013) e Zhang, Liu e Xu (2015). Todos estes efeitos ligados a escala, que operam conjuntamente no caso das plataformas digitais, favorecem a concentração de mercado e o fortalecimento de posições dominantes, tornando-a entrincheirada e dificultando o ataque de concorrentes atuais e potenciais. Agora, os governos começam a chegar a essa conclusão, como fica evidente, por exemplo no relatório sobre Legislação Antitruste 4.0, elaborado pelo Ministério de Assuntos Econômicos e de Energia da Alemanha, já citado na Seção 3.1.2.1.

A expansão dessas plataformas, aliada à grande geração de excedente, que pode ser utilizado para promover o crescimento artificial a partir de aquisições, permite que estas empresas, na ausência de sistemas eficientes de regulação da concorrência, possam aumentar suas ramificações de capilaridade física e lógica, tornando-se ainda mais eficientes na captação de dados pessoais, o que aumenta o poder e a eficiência de seus sistemas de perfilização. Quanto mais dados pessoais captados, mais ampla se torna a rede de vigilância, maior será a capacidade de segmentação de mercado - a busca pelo mercado de um, apresentada na Seção 3.1.1 - e menor será o excedente do consumidor nas relações intermediadas pelas plataformas. Direitos Fundamentais, que deveriam ser protegidos pelo uso controlado dos dados pessoais, e direitos do consumidor, que deveriam ser garantidos em detrimento de vantagens excessivas dos fornecedores, são simultaneamente violados.

Nesse ponto, tendo observado as fragilidades das legislações de proteção de dados pessoais de matriz europeia, abordadas na Seção 4.1.2, para lidar com os desafios de aumentar o nível de proteção quando se está diante de uma plataforma digital global, que concentra grande volume de dados, com ultra capilaridade e imenso poder computacional, a conexão mais intensa e a articulação conjunta da própria legislação de proteção de dados e dos arcabouços legislativo e regulatório do Direito Concorrencial e do Direito do Consumidor, passam a fazer enorme sentido.

De plano, é preciso reconhecer que estes dois últimos campos estão ligados no contexto normativo brasileiro. O vínculo se dá por força constitucional, tendo em vista que, juntas, livre concorrência e defesa do consumidor, figuram como princípios da proteção constitucional à ordem econômica (art. 170, IV e V, da Constituição Federal). Há um diálogo de fontes evidente e referências explícitas a institutos de um campo na legislação do outro e vice-versa. Já no art. 1º, da Lei 12.529/2011, a defesa dos consumidores figura como princípio orientador do Sistema Brasileiro de Defesa da Concorrência. Na aplicação das penas às infrações à ordem econômica, a lei também estabelece como parâmetro o grau de lesão aos consumidores (BRASIL, 2011). Já o Código de Defesa do Consumidor (CDC), estabelece como princípio da Política Nacional das Relações de Consumo, a repressão dos “abusos praticados no mercado de consumo, inclusive a concorrência desleal” (BRASIL, 1990), elementos afeitos à



defesa da concorrência. A importância dessa ação conjunta, especificamente no âmbito digital, vem sendo apontada pela doutrina já há algum tempo. Em 2012, Bruno Miragem, por exemplo, alertava:

Ademais, porque atualmente a intervenção do Estado no domínio econômico em matéria de defesa da livre concorrência e dos consumidores, é desafiada em muitos setores, mas especialmente no da chamada nova economia, relativa aos serviços informáticos e de Internet, por iniciativas e condutas dos agentes de mercado que resultam na aproximação cada vez maior entre as políticas antitruste e de defesa do consumidor. (MIRAGEM, 2012)

Como exposto na Seção 2.1, na economia de dados, que começa a moldar uma sociedade da vigilância, grandes massas de dados são capturadas em relações de consumo de diversas naturezas, processadas por estruturas computacionais gigantescas, controladas por um número bastante pequeno de empresas, mas operadas por múltiplos players, de diversos tamanhos, em ramificações hiper conectadas. Consequentemente, com os novos arranjos econômicos, a proteção do consumidor, os esforços de incentivo à competição e a proteção de dados pessoais precisam se unir não apenas porque todo esforço para garantir a eficácia dos Direitos Fundamentais é bem vindo, mas principalmente porque esses mesmos arranjos, na prática, se engendram de modo a vulnerar os elementos essenciais que cada uma dessas áreas se destina a proteger.

#### 4.2.1 A simbiose entre Proteção à Concorrência e Proteção de Dados Pessoais

Em decisão de 16 de fevereiro de 2019, a autoridade alemã de defesa da competição, Bundeskartellamt, proibiu o Facebook, nos casos em que sua rede social, designada por Facebook.com, é acessada por usuários residentes na Alemanha que usam outros aplicativos de sua propriedade - WhatsApp, Oculus, Masquerade, Instagram -, de coletar os dados dos usuários e dos seus dispositivos e integrá-los a partir dessas aplicações, vinculando-os a uma única conta, sem o consentimento do usuário (Parte 1 da decisão<sup>33</sup>). A mesma vedação se aplica aos termos que permitem que o Facebook combine informações salvas, na Conta Facebook, com informações coletadas a partir de interfaces de programação - as APIs, tratadas na Seção 2.1.2 -, no caso específico as *Facebook Business Tools*, utilizadas em websites e em aplicativos de terceiros, sem o consentimento do usuário (Parte 2). A base legal da decisão é a Seção 19(1) da Lei de Competição da Alemanha (GWB), que determina que “[o] abuso de uma posição dominante por uma ou várias empresas é proibido”<sup>34</sup> (GERMAN, 2013). A autoridade alemã também decide que não há consentimento válido para que os dados

<sup>33</sup> A divisão em Parte 1 e Parte 2 é utilizada apenas para facilitar o detalhamento dos efeitos e as consequências de cada uma das partes.

<sup>34</sup> No original: “The abuse of a dominant position by one or several undertakings is prohibited.” (tradução livre)

dos usuários sejam coletados se esse consentimento é um pré-requisito para o uso da plataforma. Todas as informações da decisão, apresentadas até agora, foram extraídas do Resumo do Caso, emitido pela própria Bundeskartellamt (2019).

Na Parte 1, a autoridade alemã impõe a barreira do consentimento como necessária para que o Facebook possa integrar em uma mesma base, dados vindos de duas ou mais plataformas de sua propriedade. A troca de dados dentro da família de empresas e produtos do Facebook foi tratada na Seção 3.1.1, para exemplificar a importância dos metadados, inclusive explicitando o poder dessa integração em termos de segmentação de publicidade, com o caso da comida vegana. Com essa imposição, a autoridade age para que o usuário tenha a possibilidade de barrar um tipo de integração de dados que aumenta o potencial de vigilância e a acurácia da perfilização à qual estará submetido. Também cria uma barreira para o efeito de escala de dados, uma externalidade positiva aproveitada pela plataforma e que facilita seu entrenchamento em uma posição dominante ou monopolística, dificultando a entrada de outros *players* no mercado.

Já a Parte 2 busca mitigar, com o mesmo expediente de imposição da barreira do consentimento, os efeitos das integrações automáticas de dados, originados em páginas e aplicações de terceiros, realizadas via API. É uma atuação direta para aplacar a capilaridade lógica da plataforma<sup>35</sup>. Em ambos os casos, age contra conduta de abuso de posição dominante, que fere a autodeterminação informativa por não proporcionar ao indivíduo o direito de decidir, livremente e sem qualquer tipo de coerção, sobre o modo como os seus dados são processados.

Vale lembrar que, em julho de 2017, entrou em vigor, na Alemanha, a nona alteração da lei antitruste do país. Com ela, os efeitos de escala, incluindo os efeitos de rede, o acesso a dados relevantes para a competição e a pressão competitiva orientada a dados, além dos produtos e serviços oferecidos sem pagamento direto, em dinheiro, passaram a incorporar o texto legal (GERMAN, 2013):

§ 18. Dominância de Mercado

(...)

(2a) A presunção de um mercado não deve ser invalidada pelo fato de um bem ou serviço ser fornecido gratuitamente.

(...)

(3a) Em especial no caso de mercados e redes de múltiplos lados, na avaliação da posição de mercado de uma empresa também devem ser considerados: 1. os efeitos de rede diretos e indiretos, 2. a utilização paralela de serviços de diferentes fornecedores e os custos de troca para os usuários, 3. as economias de escala do competidor decorrentes de efeitos de rede, 4. o acesso do competidor a dados relevantes para a concorrência, 5. a pressão competitiva orientada a inovação.<sup>36</sup>

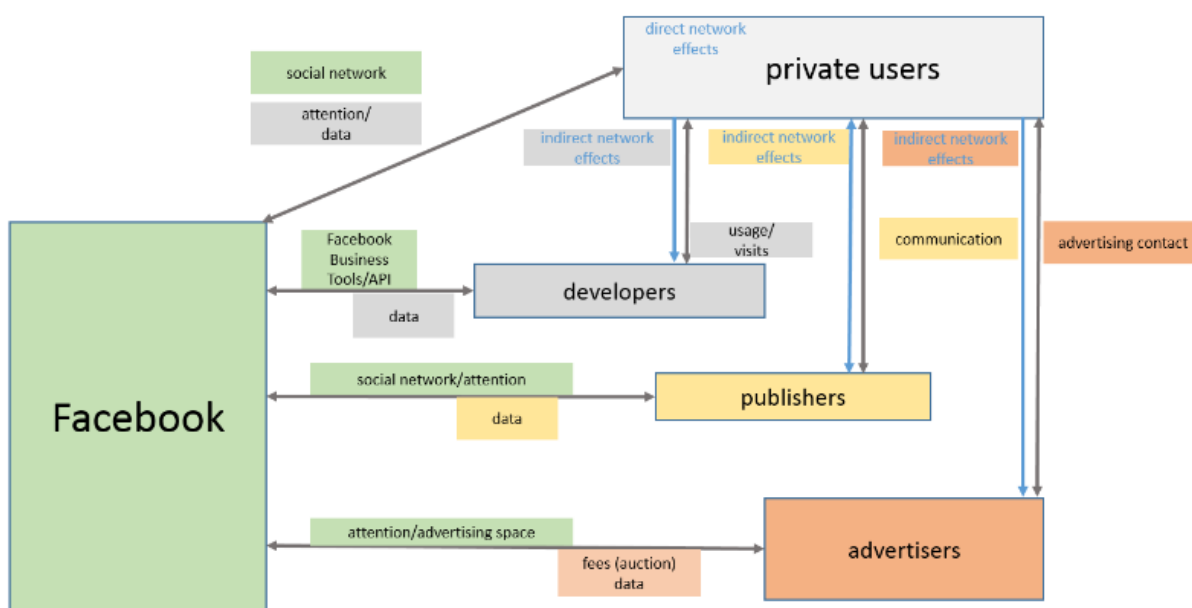
<sup>35</sup> Sobre capilaridade lógica, ver Seção 2.1.2).

<sup>36</sup> No original: “§ 18. Market Dominance (...) (2a) The assumption of a market shall not be invalidated by the fact that a good or service is provided free of charge. (...) (3a) In particular in the case of multi-

A opção da Alemanha, ao incluir na sua lei antitruste esses elementos, que ajudam a caracterizar uma posição dominante na economia orientada a dados, demonstra como é fundamental um entendimento preciso desses conceitos. Fazendo um paralelo com o Brasil, a ausência de previsão desses elementos não impede que eles sejam analisados pela autoridade de proteção à concorrência, mas melhor caminhariam os processos se estes fatores estivessem positivados, pois, assim, a análise desses fatores deixaria de ser uma faculdade e passaria a ser uma obrigação legal.

Retomando o caso alemão, para explicitar todos esses efeitos, a Bundeskartellamt (2019) apresentou, no Resumo do Caso, um diagrama, mostrado a seguir, expondo as relações entre os diversos lados da oferta do Facebook, que envolve os usuários, os desenvolvedores (que integram elementos do Facebook, via API, em seus websites e aplicativos), os publishers (que utilizam as *fanpages* para se comunicarem com seus públicos de interesse) e os anunciantes (empresas que pagam para que os usuários possam visualizar suas publicações).

Figura 5 – Diagrama de interação entre os múltiplos lados, no modelo de negócio do Facebook



Fonte: Bundeskartellamt

A figura indica um efeito direto de rede, dentro do elemento *private users*, apenas para lembrar que redes sociais geram um efeito de rede direto, já que, com o aumento do número de pessoas que aderem à rede mais pessoas se interessam por aderir. Já

sidéd markets and networks, in assessing the market position of an undertaking account shall also be taken of: 1. direct and indirect network effects, 2. the parallel use of services from different providers and the switching costs for users, 3. the undertaking's economies of scale arising in connection with network effects, 4. the undertaking's access to data relevant for competition, 5. innovation-driven competitive pressure." (tradução livre)

os efeitos de rede indiretos estão presentes em todos os negócios de dois ou múltiplos lados, a partir do momento em que se atinge, obviamente, a massa crítica necessária para desencadear o efeito. O diagrama aponta efeitos de rede indiretos de usuários privados para anunciantes (quanto mais usuários aderem à rede, mais anunciantes se interessam por anunciar na plataforma), entre usuários privados e desenvolvedores (quanto mais usuários, mais os desenvolvedores se interessam em utilizar as APIs da plataforma), e um efeito de rede indireto duplo na relação entre usuários privados e *publishers*. O diagrama também indica a relação de troca entre os usuários, que acessam a rede social, e o Facebook, que recebe deles atenção e dados pessoais. Já na relação entre anunciantes e Facebook, os dados de lance para os leilões, são enviados pelo anunciante que, em contrapartida, recebe do Facebook os espaços publicitários e a atenção dos usuários.

Alguns aspectos da decisão merecem comentários específicos. O primeiro diz respeito à relação entre modelo de negócio e fonte de dados:

redes sociais financiadas por publicidade geralmente precisam processar grandes volumes de dados pessoais. Porém, a Bundeskartellamt sustenta que a eficiência do modelo de negócio baseado em publicidade personalizada não pode superar os interesses dos usuários quando se trata de processar dados de fontes externas à rede social<sup>37</sup> (BUNDESKARTELLAMT, 2019a).

A autoridade alemã reconhece como legítimo o uso de dados pessoais para sustentar os modelos de negócio baseados em publicidade, em que o usuário não oferece uma contrapartida financeira para a utilização dos serviços. Inclusive, no texto da decisão, destaca que a disponibilização de redes sociais sem contrapartida financeira, financiada por publicidade, pode ser considerado um grande benefício para os consumidores, mas há limites para a eficiência desses modelos, principalmente quando o usuário não tem controle sobre o processo utilizado para processamento dos seus dados (BUNDESKARTELLAMT, 2019b). Os limites, neste caso, também se referem à eficiência da perfilização, utilizada para entregar uma publicidade segmentada mais precisa, com maior potencial de conversão, para os anunciantes. Com a barreira do consentimento, impede-se que dados pessoais de múltiplas fontes - milhões delas - sejam automaticamente integradas ao perfil (conta) do usuário. Portanto ataca frontalmente a capilaridade lógica, uma das grandes impulsionadoras do efeito de escala de dados.

No segundo ponto, a Bundeskartellamt faz a conexão entre direito concorrencial e proteção de dados: “foi necessário intervir a partir da perspectiva do direito da concorrência porque os limites de proteção de dados, estabelecidos no GDPR, foram

<sup>37</sup> No original: “advertising-funded social network generally needs to process a large amount of personal data. However, the Bundeskartellamt holds that the efficiencies in a business model based on personalised advertising do not outweigh the interests of the users when it comes to processing data from sources outside of the social network” (tradução livre)

claramente ultrapassados, também em vista da posição dominante do Facebook”<sup>38</sup> (BUNDESKARTELLAMT, 2019a).

Aqui, fica claro que a autoridade de proteção à competição da Alemanha realiza uma intervenção que atinge o modelo de negócio, com objetivo de proteger os direitos ligados à proteção de dados dos usuários finais, em virtude da posição dominante do Facebook. A legislação antitruste é operada em favor dos Direitos Fundamentais, considerando os efeitos de rede (direto e indiretos) que favorecem o fornecedor e, adicionalmente, aumentam a vulnerabilidade do consumidor. Esse posicionamento se fundou em decisões do Tribunal Federal de Justiça alemão no sentido de que para proteção de direitos constitucionais, as previsões da Seção 19 da GWB, que trata das condutas proibidas de competidores dominantes (*prohibited conduct of dominant undertakings*), deve ser aplicada quando uma parte de um contrato é tão poderosa que praticamente dita os termos do contrato, abolindo a autonomia contratual da outra parte, sendo que, nos casos onde uma companhia dominante manipula direitos constitucionais daqueles com quem celebra contratos, a legislação de concorrência deve intervir para proteger esses direitos. (BUNDESKARTELLAMT, 2019a).

Esse entendimento, à luz da legislação antitruste brasileira e do alto grau de proteção aos Direitos Fundamentais, previsto na Constituição Federal, seria plenamente aplicável no Brasil, tendo em vista que a previsão de garantia à existência digna de todos, estabelecida no art. 170 da Constituição Federal, que absorve a ideia de maximização da eficácia dos Direitos Fundamentais, autoriza a aplicação da lei específica para esse fim. Eros Grau, ao comentar este artigo, e citando a similaridade com a Constituição da Alemanha, assevera que a dignidade humana “fundamenta e confere unidade não apenas aos direitos fundamentais - direitos individuais, direitos sociais e econômicos - mas também à organização econômica” (GRAU, 2018). Nesse sentido, autoriza-se a ação, pela via da defesa da concorrência, influenciando na organização econômica, para aumentar a eficácia dos Direitos Fundamentais. Fecha-se, assim, um ciclo de proteção.

Um terceiro trecho deixa claro que a decisão levou em conta, também, os efeitos de escala do lado da produção:

O Facebook também tem excelente acesso a dados competitivamente relevantes. As fontes de dados abrangentes do Facebook são altamente relevantes para fins de concorrência, pois uma rede social é impulsionada por esses dados pessoais. Além disso, esses dados específicos facilitam a publicidade altamente personalizada. Combinado com os efeitos diretos e indiretos da rede, esse acesso aos dados constitui outra barreira de entrada para produtos de concorrentes que pode ser monetizada<sup>39</sup> (BUNDESKARTELLAMT,

<sup>38</sup> No original: “it was necessary to intervene from a competition law perspective because the data protection boundaries set forth in the GDPR were clearly overstepped, also in view of Facebook’s dominant position.” (tradução livre)

<sup>39</sup> No original: “Facebook also has excellent access to competitively relevant data. Facebook’s comprehensive data sources are highly relevant for competition as a social network is driven by such

2019a).

Como detalhado na Seção 3.1.2.2, os efeitos de rede, direto e indireto, não são as únicas externalidades positivas aproveitadas pelas plataformas. A externalidade do lado da produção, ligada à escala de dados, também pode colaborar com a concentração de mercado. Intensificar esse efeito, muitas vezes artificialmente, como no caso da previsão contratual que obriga o usuário a aceitar a integração de dados obtidos por diversos produtos e, também, a partir de websites e aplicativos de terceiros, pode, e muitas vezes significa, um ato de concorrência desleal e de abuso de posição dominante. Esse reconhecimento é importante, porque aponta para os impactos à concorrência da economia da vigilância, tendo em vista que “publicidade altamente personalizada” é sinônimo de mecanismos também altamente eficientes de perfilização, que buscam chegar próximo do ideal mercado de um.

A decisão também explícita, observada do ângulo inverso, a concordância da autoridade alemã com a troca realizada entre Facebook e usuários, onde estes últimos recebem acesso à rede social e, em retribuição, disponibilizam dados pessoais e atenção. Desviando-se da questão sobre o uso de dados pessoais como moeda de troca, a decisão expõe, no parágrafo 379 (BUNDESKARTELLAMT, 2019b):

Em particular no caso de plataformas de Internet financiadas por publicidade, em que os pagamentos monetários diretos pelos usuários dos serviços são substituídos pela comercialização da atenção e dos dados do usuário, para os anunciantes, na forma de publicidade direcionada, o escopo de processamento de seus dados, que os usuários não podem evitar por causa do poder de mercado dos serviços, também é um fator relevante na definição do poder de mercado. Isso se aplica independentemente da questão de saber se os próprios dados do usuário devem ser considerados como pagamento por um serviço ou como uma condição contratual que serve para manter um preço zero<sup>40</sup>.

Ao limitar o escopo, exigindo o consentimento para dados gerados fora da plataforma principal (Facebook.com), seja a partir de aplicações de sua propriedade (parte 1 da decisão), seja pela integração com sites e aplicativos de terceiros (parte 2), no sentido contrário, delimita um universo de dados cujo tratamento é autorizado como contrapartida pela utilização da plataforma. A Bundeskartellamt alinha-se, então, à Diretiva 2019/770 que reconhece essa relação de troca envolvendo fornecimento

personal data. In addition, these specific data facilitate highly personalised advertising. Combined with the direct and indirect network effects, this access to data constitutes another barrier to market entry for a competitor's product that can be monetised.” (tradução livre)

<sup>40</sup> No original: “In particular in the case of advertising-funded internet platforms, where direct monetary payments by users of the services are replaced by attention marketing and the marketing of user data to advertisers in the form of targeted advertising, the scope for processing user data which users cannot avoid because of the services' market power, is also a relevant factor in defining market power. This applies irrespective of the question of whether the user data themselves are to be considered as payment for a service or as a contractual condition serving to maintain a price of zero.” (tradução livre)

de dados em contrapartida a acesso de serviços digitais, apesar de também tentar esconder, não na forma de dúvida, como fez a autoridade alemã, mas pelo uso de eufemismos, seu caráter transacional.

Ainda neste trecho, a Bundeskartellamt também reconhece a apropriação do tempo dos usuários, tratado na Seção 2.2.3, como parte da entrega da plataforma aos anunciantes, designando-a de marketing de atenção. Assim, a decisão tenta proteger o indivíduo, simultaneamente, nas três posições que ocupa ao utilizar uma plataforma digital: como consumidor, ao buscar minimizar os efeitos de concentração de mercado, aumentando as chances de entrada para novos competidores; como fornecedor de matéria-prima, ao limitar o escopo dos dados tratados como contraprestação à disponibilização dos serviços e como alvo da publicidade (produto, na acepção utilizada na Seção 3.3) por considerar também esse elemento como contrapartida pelo uso, na relação usuário-Facebook, e entrega final, junto com os espaços publicitários, na relação Facebook-anunciante.

Um último aspecto a ser abordado diz respeito à diferença radical entre a decisão da Bundeskartellamt, neste caso, e aquela proferida pelo Tribunal de Justiça da União Europeia, contra a Fashion ID, que envolve a mesma situação de captação de dados a partir de sites externos à rede social, a partir de integração via APIs (*Facebook Business Tools*) e que foi abordada na Seção 4.1.2.2. Enquanto, na decisão do Tribunal Europeu, multiplicou-se a responsabilização, fragmentando a barreira do consentimento para todos os sites e aplicações que utilizam as APIs do Facebook, na decisão alemã a responsabilização fica concentrada no player que detém a posição dominante e que, efetivamente, pode abusar dessa posição e colocar em risco os Direitos Fundamentais dos usuários. Além disso, a solução alemã não impõe um ônus adicional a pequenos *players*, de diversos mercados, que utilizam as ferramentas de integração do Facebook para melhorar a comunicação com seus públicos-alvo, derivado de mais um item de consentimento. Também cria um ônus administrável para os usuários, que terão que controlar, em um único ponto, o nível de exposição à qual desejam ficar submetidos, ao contrário da solução encontrada pelo tribunal europeu, que acabará forçando o indivíduo a tomar micro-decisões de consentimento, em cada site ou aplicação que acessar. A dificuldade de decidir sobre como fazer a alocação de disponibilidade dos seus dados também é outro aspecto que importa comentar. Como visto na Seção 3.1.1, decisões sobre privacidade possuem peculiaridades importantes e o usuário muitas vezes não consegue visualizar com clareza os riscos e as perdas envolvidas na cessão de seus dados pessoais para terceiros. Ao diluir o consentimento, essa dificuldade tende a aumentar, porque ao autorizar, individualmente, a captação e tratamento dos seus dados, o usuário, na maioria das vezes, não conseguirá enxergar que, da soma de todas as suas autorizações, poderá nascer um sistema de vigilância, enquanto em um sistema de barreira de consentimento central, onde o usuário

se confronta com uma grande empresa, essa sensação de vigilância se torna mais perceptível.

Essa comparação entre as decisões também permite perceber que abordar ou não os efeitos de rede e de escala, levando-os em consideração, pode definir o rumo da regulação e da atuação estatal, seja no âmbito administrativo, seja nos Tribunais.

#### 4.2.1.1 Novos parâmetros para a proteção à competição

A alteração promovida na legislação de proteção à competição da Alemanha é um bom indicativo de como essa categoria de leis tenderá a mudar nos próximos anos. Em matéria no *The Wall Street Journal*, que trata do endurecimento das autoridades antitruste contra as Big Techs, um representante do Facebook, que não se identificou, classificou a decisão da Bundeskartellamt como “não convencional” (OLSON, 2020). Como discutido anteriormente, a autoridade alemã aponta sua atuação para uma direção diferente da tradicional, que é baseada em uma leitura linear da GDPR, sem considerar os aspectos econômicos, como os efeitos de rede que são aproveitados pelas plataformas para reforçar suas posições de dominância de mercado.

Apesar de não ortodoxa, a decisão parece se alinhar à percepção mais ampla, de que os parâmetros utilizados para avaliação da competição no mundo das plataformas precisa ser diferente daqueles utilizados nos mercados tradicionais. Em dezembro de 2019, o Fórum Econômico Mundial publicou um relatório sobre políticas de competição, com foco na economia digital, contendo dez recomendações. Três delas merecem destaque. A primeira sugere que, na regulação da concorrência envolvendo plataformas, não existe solução *one size fits all*<sup>41</sup>. Nesse ponto, reforça a ideia de que plataformas não são estruturas monolíticas, que funcionam sempre da mesma forma em diferentes mercados e com o mesmo modelo de negócio. Além disso, os órgãos de controle precisam aumentar seus níveis de conhecimento em análise de dados e algoritmos, investindo no desenvolvimento de aplicações que monitorem as atividades de mercado e ajudem a desenhar respostas efetivas, o que poderá resultar na criação de unidades de tecnologia dentro dos órgãos de controle (WORLD ECONOMIC FORUM, 2019). A segunda indica que as ferramentas utilizadas pelas legislações de proteção à concorrência precisam ser repensadas. A necessidade de se considerar os modelos de múltiplos lados e os efeitos de rede, que levam não para uma competição no mercado, mas a uma competição pelo mercado; observar a importância dos dados na definição dos mercados relevantes; de analisar o grau de influência e os esforços de inovação no cenário competitivo e de avaliar a importância dos resultados gerados por máquina, são alguns elementos a considerar. Já a terceira recomendação destaca a ideia de que as leis antitruste devem ser operadas para que a proteção à competição possa trazer benefícios para os cidadãos enquanto consumidores, neste

<sup>41</sup> Numa tradução livre: “uma solução que vale para todos os casos”



sentido “[o] bem-estar do consumidor deve ser considerado uma base fundamental para um esforço de cooperação internacional relacionado a ações de *enforcement* envolvendo a dinâmica das companhias multinacionais no mercado global”<sup>42</sup> (WORLD ECONOMIC FORUM, 2019), destaca o relatório.

As mudanças também são impulsionadas pelos governos. Buscando dar um passo a frente, em setembro de 2019, uma comissão montada pelo Ministério de Assuntos Econômicos e Energia da Alemanha, apresentou relatório (COMMISSION ‘COMPETITION LAW 4.0’, 2019) que delinea recomendações para uma nova regulamentação europeia para a competição, no sentido de torná-la mais eficiente nos mercados que envolvem a economia digital e as plataformas. Visto como um ponto central, o documento sugere o fortalecimento da autonomia como forma de facilitar o acesso aos dados e evitar problemas que afetam a competição, dedicando um dos seus dez capítulos a esse tema. Com uma visão mais ampla, neste capítulo há um item específico que aborda a questão dos dados pessoais. Nele, a Comissão apresenta três recomendações:

(1) fortalecimento dos direitos do consumidor à portabilidade de dados, especialmente em relação às empresas dominantes; (2) estabelecimento de regimes de acesso a dados em uma base específica e setorial, que permita aos consumidores conceder a terceiros acesso a suas contas de usuário; (3) examinar se, e em que circunstâncias, o estabelecimento de novos “custodiantes de dados” - ou seja, instituições que aplicam preferências de uso de dados em nome dos consumidores, individual e coletivamente, e também oferecem acesso conjunto às empresas a esses dados para os fins para com os quais os consumidores concordaram - podem aprimorar tanto a capacidade dos consumidores de determinar como os “seus” dados são processados, quanto fortalecer a concorrência e as possibilidades de inovação orientada a dados<sup>43</sup> (COMMISSION ‘COMPETITION LAW 4.0’, 2019).

Seguindo esta visão baseada na fluidez do acesso, o relatório pondera que o direito à portabilidade, da maneira como foi estruturado no artigo 20 da GDPR<sup>44</sup>, atua

<sup>42</sup> No original: “Consumer welfare can also provide a foundational basis for international cooperation efforts regarding enforcement actions involving multinational businesses in dynamic, global markets.” (tradução livre)

<sup>43</sup> No original: “(1) strengthening consumer rights to data portability, particularly vis-à-vis dominant companies; (2) establishing data access regimes on a sector-specific and selective basis which enable consumers to give third parties access to their user accounts; (3) examining whether and under what circumstances the establishment of new “data trustees” – i.e. institutions which enforce data usage preferences on behalf of consumers both individually and collectively and also offer pooled access for companies to such data for the purposes to which the consumers have agreed – can enhance both the ability of consumers to determine how “their” data are processed and strengthen competition and the possibilities for data-driven innovation.” (tradução livre)

<sup>44</sup> Artigo 20.o - Direito de portabilidade dos dados

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:

a) O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e

na migração de dados, de uma plataforma para outra, auxiliando em um movimento de substituição. Não seria adequado, portanto, para situações de transferência em tempo real (*ongoing real-time transfers*). Também apresenta a fragilidade do direito à portabilidade quanto aos dados contextuais, gerados a partir da interação com outros indivíduos (tema tratado na Seção 2.3.2). Também critica a previsão legal da portabilidade pela definição precária quanto a formatos técnicos para implementação desse direito, indicando que a previsão de formato interoperável aparece apenas em um recital e não no texto cogente. O relatório também conclui que, apesar das dificuldades de implementação e das limitações quanto à utilidade prática do direito à portabilidade, uma exigência legal que imponha um direito de interoperabilidade, permitindo a transferência em tempo real de dados para concorrentes e provedores de serviços complementares, acarretaria custos adicionais que serviriam como novas barreiras de entrada para competidores, principalmente para os de menor porte. Também pode gerar um efeito colateral relevante, já que os indivíduos podem achar interessante integrar os dados armazenados em aplicações de pequenos fornecedores aos serviços e bancos de dados dos grandes *players*, aumentando ainda mais a concentração dos dados. Neste contexto, a Comissão recomenda a imposição, às plataformas dominantes, de prover mecanismos de interoperabilidade e de acesso, em tempo real, aos dados, para integração (COMMISSION ‘COMPETITION LAW 4.0’, 2019). Aqui, a Comissão, em certa medida, maneja a autodeterminação informativa, colocando-a com um papel duplo. Primeiro como forma de garantir a autonomia do indivíduo no manejo dos seus dados pessoais. Segundo, como um gatilho para viabilizar o fluxo de dados entre aplicações. Mais uma vez, aponta-se para o indivíduo na alocação da responsabilidade sobre a forma de utilização dos seus dados. Apesar de essa ser uma consequência inescapável da autonomia para dispor dos seus dados, não se pode perder de vista todas as dificuldades relativas à tomada de decisão relacionadas ao compartilhamento de dados, que se tornam tão maiores quanto maior a complexidade da tecnologia utilizada e do emaranhado de aplicações interconectadas necessárias para disponibilização de um serviço digital.

Outro ponto relevante trazido pelo relatório refere-se à possibilidade de acesso de terceiros a contas de dados. Utiliza, para isso, o exemplo do *open banking*<sup>45</sup>, que

b) O tratamento for realizado por meios automatizados.

2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.

3. O exercício do direito a que se refere o n.º 1 do presente artigo aplica-se sem prejuízo do artigo 17.º. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.

4. O direito a que se refere o n.º 1 não prejudica os direitos e as liberdades de terceiros.

<sup>45</sup> Em resumidíssima síntese, *open banking* relaciona-se com a disponibilização, por instituições financeiras, para outros provedores de serviços, bancários ou não bancários (fintechs, seguradoras, varejistas etc), de acesso a informações financeiras de clientes, a partir de APIs. (CHAPPELOW, 2019)

possibilita que *fintechs* prestem serviços para usuários finais integrando dados a partir de instituições financeiras, o que envolve questões relevantes relacionadas a segurança e proteção de dados. Sugere neste caso que, além da formulação de princípios gerais para acesso a contas de dados, a Comissão Europeia tenha autorização para aprofundar a regularização, baseado em setores específicos (COMMISSION ‘COMPETITION LAW 4.0’, 2019). Se por um lado a ideia de acesso a contas de dados aumenta a flexibilidade e o poder dos indivíduos de utilizarem diversos serviços que operam com os seus dados, há uma abertura bastante expressiva para novos pontos de vulnerabilidade. Estes riscos tendem a ganhar uma magnitude ainda maior com o avanço da IoT. Vale lembrar que a criptomoeda *lota* foi desenvolvida especificamente com o objetivo de diminuir o custo das transações que envolvem dados gerados pela IoT (assunto tratado na Seção 2.1.3). Ao indicar a necessidade de regulações específicas, por setor, as recomendações da Comissão alemã e do Fórum Econômico Mundial se alinham. Realmente, não há uma solução que valha para todos os casos, mas é necessário considerar que poucos setores da economia são tão regulados quanto o mercado financeiro, onde os *players* naturalmente já contam com um porte robusto o suficiente para suportar regulações mais restritivas. Uma alternativa, levando em consideração que, atualmente, os competidores que operam no mercado financeiro são essencialmente empresas de tecnologia da informação, e que grandes concentradores de poder computacional também são capazes de suportar maior pressão regulatória, seria o estabelecimento de regulações específicas não apenas para setores da economia, mas também por famílias de tecnologias, com imposições técnicas, no sentido de uma outra sugestão do Fórum Econômico Mundial, apresentada anteriormente, e também aproveitando-se do conceito de design e engenharia de direitos, descrito na Seção 4.1.1.

Por fim, na abordagem dada especificamente aos dados pessoais, o relatório detalha a ideia do estabelecimento de “custodiantes de dados”. Começa a abordagem do tema apontando o consentimento como um fator chave de justificação do tratamento de dados pessoais e indicando que a GDPR não deixa claro os contornos do consentimento informado e voluntário, nem resolve os “conhecidos problemas da apatia racional dos titulares de dados ao consentir com as frequentemente complexas políticas de tratamento de dados e a falta de poder do indivíduo em negociar com empresas cuja atratividade pode derivar de fortes efeitos positivos na rede<sup>46</sup>” (COMMISSION ‘COMPETITION LAW 4.0’, 2019). A Comissão também reconhece que uma política, como a sugerida, de intensificação da portabilidade e de abertura de dados de contas de usuário, pode exigir um grande esforço do indivíduo em gestão de consentimento a partir de um grande número de termos de uso de dados pessoais, o que gera

<sup>46</sup> well-known problems of the rational apathy of data subjects when consenting to what frequently will be complex data processing policies and the lack of power on the part of the individual to negotiate with companies, the attractiveness of which may derive from strong positive network effects.

limitações práticas importantes ao modelo sugerido (COMMISSION 'COMPETITION LAW 4.0', 2019).

Sistemas de Gerenciamento de Informações Pessoais (PIMS) já existem e, inclusive, já foram alvo de parecer da Autoridade Europeia de Proteção de Dados (EDPS), em 2016, que considera estas novas tecnologias como um avanço, que apoiam os indivíduos no processo de decisão de alocação de seus dados.

O conceito de PIMS<sup>47</sup> oferece uma nova abordagem onde os indivíduos são os detentores de suas próprias informações pessoais. Isso pode criar uma mudança de paradigma no gerenciamento e processamento de dados pessoais, com consequências sociais e econômicas. Por outro lado, o cenário atual dos serviços online é caracterizado por um pequeno número de provedores de serviços que dominam o mercado, monetizando os dados pessoais dos usuários que os troca por serviços "gratuitos". Isso geralmente é acompanhado de um desequilíbrio de poder, em que o cliente é submetido a uma abordagem de 'pegar ou largar', e de uma assimetria de informação entre prestadores de serviços e usuários, com pouca ou nenhuma transparência para os indivíduos sobre o que está acontecendo com seus dados pessoais<sup>48</sup> (EUROPEAN DATA PROTECTION SUPERVISOR, 2016).

Neste ponto, é importante notar que a própria autoridade europeia de proteção de dados reconhece a existência de uma troca de dados pessoais por serviços e que esses dados são monetizados, ou seja, reconhece o caráter transacional da cessão de dados pessoais. Assim, os PIMSs poderiam contribuir para mudar essa realidade, colocando o indivíduo no controle. Doc Searls (2012) faz uma analogia interessante: nos últimos tempos, as áreas de marketing e de vendas das empresas passaram a adotar abordagens mais sociais e de estabelecimento de diálogo, mas, mesmo assim, continuam enxergando os consumidores como um ativo a ser gerenciado. Para isso, as empresas têm a disposição os sistemas de Customer Relationship Management (CRM). Virar o jogo e colocar o consumidor no comando também exigiria um sistema, onde o próprio indivíduo gerenciasse as suas informações compartilhadas com cada empresa. Seria necessário, portanto, um Vendor Relationship Management (VRM), operado pelo consumidor e que poderia ser integrado com os CRMs das empresas com as quais o indivíduo gostaria de trocar informações.

Os PIMSs parecem ser uma abordagem tecnológica interessante para o problema da complexa rede de gestão de consentimento, como aponta a própria Autori-

<sup>47</sup> No parecer, a EDPS aponta a existência de outros conceitos relacionados, como *personal data stores*, *personal data spaces* e *personal data vaults*, mas que optou por PIMS por considerar a designação que melhor descreve o conceito e, também, por ser de mais fácil entendimento. No documento original, esta explicação encontra-se na nota número 7.

<sup>48</sup> No original: "The PIMS concept offers a new approach by which individuals are the holders of their own personal information. It may create a paradigm shift in personal data management and processing, with social and economic consequences. In contrast, the current landscape of online services is characterised by a small number of service providers that dominate the market by monetising users' personal data in exchange for 'free' services. This is often accompanied by an imbalance of power, where the customer is left with a 'take it or leave it' approach, and by information asymmetry between service providers and users, with little or no transparency for the individuals on what is going on with their personal data." (tradução livre)

dade Europeia de Proteção de Dados, principalmente ao se considerar a tendência de aumento da importância dos fluxos de dados pessoais no futuro. Mas o relatório da Comissão alemã vai ainda mais longe. Sugere a existência de um intermediário custodiante, que pudesse fazer, a partir das configurações do usuário, a intermediação de acesso envolvendo múltiplos titulares. Assim, o intermediário poderia agir em nome e no interesse dos seus usuários, com poder de barganha significativamente maior do que a de um titular individual, negociando melhor o nível de proteção a ser exigido do fornecedor. O próprio relatório reconhece que o tema ainda precisa ser mais amplamente discutido, sendo que os próprios PIMs poderiam ocupar a posição de custodiantes. Também indica a necessidade de uma regulação específica para custodiantes, já que acumularão um grande volume de dados pessoais e, também, para evitar que novas posições dominantes apareçam (COMMISSION 'COMPETITION LAW 4.0', 2019). Trata-se de proposta ousada que, de um lado, quebra definitivamente com o conceito monobloco de proteção de dados pessoais como Direito Fundamental e cria verdadeiros *brokers* de dados pessoais, já de outro, coloca a dúvida sobre quem vigia o vigia. Atualmente, como já abordado anteriormente, o *enforcement* eficaz é um dos maiores problemas relacionados às normas de proteção de dados pessoais. A criação de *players* administradores não diminuiria esses problemas. Além disso, a própria arquitetura da internet é aberta e descentralizada, ou seja, criar pontos de centralização que canalizam fluxos de dados não parece ser, tecnicamente, a melhor alternativa.

Os relatórios do Fórum Econômico Mundial e do Comitê Competição 4.0, da Alemanha, apresentam duas visões distintas sobre o problema da regulação da concorrência, que levam em consideração os dados pessoais como um ativo imprescindível à nova economia e a necessidade de proteção das pessoas e de seus Direitos Fundamentais. Enquanto, no primeiro, são apresentadas recomendações de implementação mais imediata, considerando inclusive alternativas já adotadas por alguns países, como a Alemanha na questão da incorporação da análise dos efeitos de rede e de escala de dados nos processos de avaliação de violações à concorrência, no segundo avança-se rumo a uma perspectiva futura. O relatório alemão tem o grande mérito de trazer temas que serão cada vez mais relevantes nas análises regulatórias envolvendo mercados baseados em dados. Também não deixa esquecer que, simultaneamente à necessidade de aumentar a eficácia dos Direitos Fundamentais a partir da proteção dos dados pessoais, ocorre um aumento da importância econômica dos fluxos de dados e a intensificação desses mesmos fluxos, que tendem a crescer exponencialmente com o avanço, por exemplo, da IoT. É sempre bom lembrar que a Lei de Moore favorece o fluxo de dados e que os modelos jurídicos adotados hoje poderão não ter lugar, por completa ineficácia, no mundo do próximo ciclo tecnológico.

#### 4.2.2 Direito do Consumidor e seu papel na extensão da proteção dos Direitos Fundamentais

O bem estar do consumidor como uma categoria relevante a ser considerada nos processos que envolvem violações à livre concorrência passa por uma revisão, no momento em que novos parâmetros precisam ser definidos para tornar a regulação aplicável às *Big Techs*, com percepções distintas dos dois lados do atlântico norte. Enquanto na Europa, o bem estar do consumidor continua mantendo um papel central, definida, inclusive, como objetivo a ser perseguido pelas autoridades antitruste, nos Estados Unidos esse foco passa a ser contestado (WORLD ECONOMIC FORUM, 2019).

O Movimento New Brandeis representa um polo de contestação. Na academia, Tim Wu, Luigi Zingales e Lina Khan, dentre outros (DOMINGUES, 2019), vêm desenvolvendo uma abordagem que dá mais ênfase às estruturas e aos processos de competição do que à ideia de bem estar do consumidor (CONIGLIO, 2018), em grande medida, contaminada pela percepção de um grande benefício proporcionado pelo preço zero. Nesse ponto, é importante delimitar o objeto designado por “bem estar do consumidor”, como alvo das críticas. Aqui, trata-se especificamente dos efeitos de preço de curto prazo. Tem-se, portanto, duas visões sobre bem estar do consumidor, esta mais direta, ligada à satisfação e seu custo (preço), e outra mais ampla, que considera o indivíduo, na posição de consumidor, e todo o seu espectro de direitos. Essa distinção, a primeira vista muito distante e desconexa, pode tornar-se paradoxal, como se demonstrará mais à frente.

O nome do movimento refere-se a Louis Brandeis, Justice da Suprema Corte americana, o mesmo que escreveu, com Samuel Warren<sup>49</sup> (1890), *The Right to Privacy*, artigo que para muitos fundou as bases do Direito à Privacidade moderno, mas que, como bem lembra Doneda (2019), não foi um feito isolado e, sim, um ponto de destaque em um ambiente onde o tema já era discutido. Apesar de tratar-se da mesma pessoa, o que vincula Louis Brandeis a esse movimento não é sua concepção de privacidade, mas seus posicionamentos quanto à regulação da concorrência, consolidada já quando ocupava uma cadeira na Suprema Corte americana, no sentido de fixar-se no que denominou de “liberdade industrial”<sup>50</sup>, que reconhecia na excessiva concentração de poder privado uma ameaça pública, fortalecendo os interesses de poucos e induzindo consequências coletivas (KHAN, 2017).

Tim Wu, um dos autores identificados com a New Brandeis School, já há tempos vem alertando para os perigos do excesso de concentração. Em 2010, escreveu um artigo de opinião sobre as empresas de tecnologia grandes demais para desaparecerem

<sup>49</sup> Louis Brandeis e Samuel Warren foram colegas no curso de Direito em Harvard e eram sócios na advocacia privada à época em que escreveram o artigo. Posteriormente, Brandeis se tornou juiz da Suprema Corte americana e Warren seguiu carreira na advocacia. (DONEDA, 2019)

<sup>50</sup> No original: “industrial liberty” (tradução livre)

dizendo que a internet se parecia com um tabuleiro de Banco Imobiliário (*Monopoly board*), onde os maiores setores eram controlados por uma única empresa ou por um oligopólio: o “[g]oogle é “dono” das buscas, o Facebook, das redes sociais; o eBay dos mercados de leilão; a Apple domina a distribuição de conteúdo online; a Amazon, o varejo, e assim vai” (WU, 2010). Contextualizando com novos players, na maioria dos casos em novos mercados, como Uber, AirBnB e Netflix, a realidade descrita por Wu não só se mantém, mas se consolidou, com players ainda mais dominantes em seus mercados principais.

Considerando uma visão eminentemente econômica de bem estar do consumidor, Khan (2017) conclui que fixar o foco nessa categoria significa estabelecer, para a análise da concorrência, uma abordagem simplista que substitui a análise da distribuição do poder de mercado, que torna o mercado competitivo, por um cálculo minimalista sobre se o preço é adequado ou alto demais. Neste sentido resume,

focar no bem-estar do consumidor desconsidera outras maneiras pelas quais a concentração excessiva pode nos prejudicar - permitindo que as empresas pressionem fornecedores e produtores, pondo em risco a estabilidade do sistema (por exemplo, permitindo que as empresas se tornem grandes demais para falir) ou minando a diversidade da mídia, apenas para citar alguns. Proteger essa gama de interesses requer uma abordagem antitruste que se concentre na neutralidade do processo competitivo e na abertura das estruturas de mercado<sup>51</sup>.

Uma abordagem ligada às estruturas que ordenam os mercados, principalmente os que envolvem dois ou múltiplos lados, tem uma relevância significativa no processo de proteção à concorrência e poder abordá-los sem o foco direto no bem estar do consumidor faz muito sentido. Um exemplo, citado por Lynskey (2019), refere-se às ações das autoridades antitruste no sentido de evitar fusões e aquisições que aumentem artificialmente os fluxos de dados controlados pelas Big Techs. Em outras palavras, as autoridades devem considerar, em suas decisões, o poder computacional e as expansões das capilaridades físicas e lógicas dos *players* envolvidos na transação.

A decisão da Bundeskartellamt mirou no mesmo objetivo: diminuir a capilaridade e os efeitos de escala de dados. Nesta decisão, também, pode-se observar a tensão existente entre os dois conceitos de bem estar do consumidor, o estreito, que se concentra no preço e satisfação, e o amplo, que considera o indivíduo na posição de consumidor. De um lado, a abordagem de entendimento dos processos de mercado, na linha do que sugere a *New Brandeis School*, foi aplicada para garantir a eficácia da GDPR como mecanismo de proteção da autodeterminação informativa, um Direito Fundamental. Aplicou-se, portanto, a visão ampla. De outro lado, a mesma decisão,

<sup>51</sup> No original: focusing on consumer welfare disregards the host of other ways that excessive concentration can harm us—enabling firms to squeeze suppliers and producers, endangering system stability (for instance, by allowing companies to become too big to fail), or undermining media diversity, to name a few. Protecting this range of interests requires an approach to antitrust that focuses on the neutrality of the competitive process and the openness of market structures. (tradução livre)

reconhece que os serviços não remunerados diretamente pelos usuários traz a eles grandes benefícios, em uma abordagem muito próxima do conceito estreito de bem estar do consumidor.

Desfazer esse paradoxo, no âmbito da regulação antitruste, pode ser um desafio quase que insuperável, o que leva à conclusão de que, muito possivelmente, não se deve apostar, quando se fala de proteção de Direitos Fundamentais no espaço das plataformas digitais, todas as fichas no Direito Concorrencial. Assim, ampliar as opções de caminho, onde a proteção à concorrência é apenas um dos atores relevantes de regulação, juntamente com outros mecanismos, como as legislações de proteção de dados e dos consumidores, parece ser mais adequado. É preciso, porém, não descuidar de sua importância, como agente de manutenção da ordem econômica, impedindo que se transforme, para utilizar uma expressão de Ezrachi e Stucke (2018), em um direito concorrencial orwelliano, “que sanciona acordos anticoncorrenciais, abusos monopolistas e maior consolidação em mercados já concentrados, tudo para promover um objetivo vago de ‘bem-estar do consumidor’”.

Como um caminho para reforço da proteção dos Direitos Fundamentais, o próprio Direito do Consumidor precisa encontrar sua posição no combate a práticas abusivas em circunstâncias que envolvem plataformas digitais. Além da proteção individual, deve assumir, como sugere Bruno Miragem (2012), sua função de ordenador do mercado de consumo, já que ao regular as relações que lhes são afetas, impõe deveres aos fornecedores, influenciando ou determinando os comportamentos dos agentes econômicos, seja por intervenção direta, seja por indução de condutas. Com isso, ao proteger o consumidor, atua na correção de falhas de mercado.

Por este prisma, mais uma vez, Direito do Consumidor, Direito Concorrencial e proteção de dados pessoais podem atuar juntos em uma equação onde o resultado é maior do que a soma das partes. Esse efeito propulsor fica evidente na desconstrução da gratuidade ilusória dos serviços oferecidos pelas plataformas digitais, a partir da análise do modelo de remuneração, que será apresentada na próxima seção.

Na sequência, o Direito do Consumidor retoma sua posição de proteção aos direitos individuais, em uma abordagem onde a proteção de dados pessoais passa a fazer parte integrante do produto ou serviço colocado em comércio, permitindo a incidência elementos normativos que garantem a qualidade.

#### 4.2.2.1 Simulacro da remuneração indireta e práticas abusivas

Historicamente, a jurisprudência no Brasil vem reafirmando que as relações de consumo estabelecidas entre os consumidores e as plataformas digitais se dão por meio de remuneração indireta. Já em 2.004, no Recurso Especial Nº 566.468 - RJ, o Ministro Jorge Scartezzini fixou entendimento neste sentido, em um caso envolvendo a divulgação indevida de nome e telefone de uma consumidora em um site de encontros



mantido pela Terra Networks Brasil.

A construção doutrinária da remuneração indireta nasce a partir da própria definição de serviço, trazida pelo CDC, que exige, para a sua caracterização, a existência de fornecimento mediante remuneração. Segundo Cláudia Lima Marques, a escolha da expressão mediante remuneração ao invés de onerosidade ou relação onerosa justifica-se, exatamente, para que se possa abarcar, nas relações de consumo, aquelas remuneradas indiretamente (BENJAMIN; MARQUES; MIRAGEM, 2019).

O que significaria esta troca entre a tradicional classificação dos negócios como “onerosos” e gratuitos por remunerados e não remunerados? Parece-me que a opção pela expressão “remunerado” significa uma importante abertura para incluir os serviços de consumo remunerados indiretamente, isto é, quando não é o consumidor individual que paga, mas a coletividade (facilidade diluída no preço de todos) ou quando ele paga indiretamente o “benefício gratuito” que está recebendo.

E completa, ao distinguir remuneração e gratuidade: “[r]emuneração” (direta ou indireta) significa um ganho direto ou indireto para o fornecedor. “Gratuidade” significa que o consumidor não “paga”.

Apesar do reconhecimento da autora de que a remuneração indireta sustenta, nos tribunais, as relações de consumo no mundo virtual, não parece ser este o enquadramento mais adequado para as relações estabelecidas entre os consumidores e as plataformas digitais utilizadas sem contrapartida pecuniária por parte do usuário.

Como apresentado em detalhes na Seção 3.2.1, os dados pessoais são, ao mesmo tempo, pequenos fragmentos que compõem a personalidade de um indivíduo e bens economicamente apreciáveis, francamente utilizados em transações e negócios jurídicos, que tem seu ápice nas plataformas digitais onde o acesso e uso é franqueado pela cessão compulsória desses dados.

Ao tratar dos direitos e garantias fundamentais ligados aos dados pessoais, na Seção 3.2.1.2, foi discutida a importância de explicitação, no texto constitucional, não apenas de uma garantia de proteção aos dados pessoais, mas também de um direito, em sentido estrito, de disposição, pelo indivíduo, dos seus próprios dados, aceitando-os como parte formadora da personalidade humana, portanto, sujeito a limitações de aproveitamento econômico, mas não vedando-a, já que isso seria simplesmente a negação de uma realidade inescapável. Voltando a olhar para o direito europeu, essa é a conclusão que pode-se extrair, inclusive, do já citado Considerando 24, da Diretiva 2019/770, que, mesmo utilizando diversos eufemismos, equipara a cessão dos dados pessoais ao pagamento de um preço para a utilização de plataformas digitais.

Nesse contexto, com um entendimento mais preciso sobre a forma de organização das plataformas digitais, principalmente sobre a utilização dos dados pessoais como matéria-prima para o fornecimento dos serviços, pelas plataformas, para seus clientes do outro lado (em geral, os anunciantes, em uma plataforma de dois lados),

fica mais fácil de enxergar que os dados pessoais utilizados, na outra ponta, como matéria-prima são, por sua vez, obtidos a partir das relações de consumo, pagas pelos usuários, com a cessão dos seus dados pessoais. Há, portanto, uma remuneração direta não pecuniária, tendo em vista que o pagamento efetuado pelo consumidor se dá a contraprestação, ou seja, no momento em que a relação de consumo acontece, no curso da prestação de serviço.

Sobre a cessão de uso dos dados pessoais como contraprestação, no âmbito das relações de consumo, o professor da Universidade de Coimbra, Alexandre Dias Pereira (2016) esclarece:

De todo o modo, é interessante registrar que nos termos da proposta os contratos de utilização de serviços informáticos à distância, como contas de correio eletrônico, redes sociais, etc., deixam de ser contratos gratuitos já que a autorização para utilização de dados pessoais é equiparada ao dinheiro para efeitos do regime contratual. Nessa medida, os dados pessoais passam a ser uma *res intra commercium*.

Outra característica importante das plataformas digitais diz respeito ao fato de que a cessão dos dados pessoais não possui relação com a prestação de serviços em si. O serviço oferecido ao consumidor continuaria hígido, do ponto de vista operacional, mesmo interrompendo-se a cessão. Muito diferente do caso dos contratos de poupança, indicado como exemplo, por Marques (BENJAMIN; MARQUES; MIRAGEM, 2019), de outra situação de remuneração indireta. No caso do poupador, a transferência dos valores para o banco faz parte da própria prestação de serviço que será remunerada, necessariamente, por um sinalagma escondido. Se, no caso dos bancos, a remuneração indireta é uma característica intrínseca da prestação dos serviços financeiros de poupança, para as plataformas, a opção por forçar a remuneração direta pela cessão de dados pessoais é uma decisão de negócio das plataformas. O que se observa, portanto, é um simulacro: uma relação baseada em remuneração direta que se esconde sob uma aparência de remuneração indireta.

Essa discussão sobre o tipo de remuneração pode parecer fútil, em um primeiro momento, mas o reconhecimento da remuneração direta dos serviços prestados pelas plataformas digitais permite estabelecer um outro debate, esse sim fundamental para os contornos dessa categoria de relação de consumo: a existência de uma relação abusiva, que obriga o consumidor a pagar pelo serviço exclusivamente por meio da cessão de seus dados pessoais.

Como já abordado, o art. 4º, VI, do CDC estabelece como princípio a “coibição e repressão eficientes de todos os abusos praticados no mercado de consumo, inclusive a concorrência desleal” (BRASIL, 1990). Mais uma vez, reforçando o diálogo das fontes e a conexão entre proteção do consumidor e da concorrência, este princípio desencadeia um amplo espectro de determinações legais, expressas no próprio código, e também estabelece a linha de atuação a ser adotada pelos órgãos estatais de prote-

ção do consumidor. Nesse quadro, são precisas as palavras de Cláudia Lima Marques (2019) ao salientar que o abuso de poder econômico deve ser coibido, em qualquer circunstância em que gerar prejuízo aos consumidores, mesmo que, eventualmente, não exista violação à Lei Antitruste.

No rol de direitos básicos do consumidor, em decorrência da repressão às práticas abusivas, o CDC (BRASIL, 1990) explicita a proteção do consumidor “contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviço” (art. 6º, IV).

Desmanchando a máscara da falsa gratuidade, a primeira violação que se torna evidente é a publicidade enganosa, o que atrai a incidência do art. 37 do CDC, sempre que uma plataforma, que exige a cessão de dados pessoais como contraprestação à disponibilização de serviços, comunica seus produtos como gratuitos. Essa é uma informação inteiramente falsa. Também induz em erro o consumidor por mascarar a existência de um preço que lhe é cobrado, diretamente, para que possa ter acesso ao serviço.

Cabe, agora, avaliar se há outras circunstâncias envolvendo métodos coercitivos ou desleais, ou ainda, práticas que possam ser consideradas abusivas.

De volta às plataformas digitais, é importante reforçar, como já destacado anteriormente, que o consumidor é forçado a aceitar a cessão de seus dados pessoais, que serão utilizados para fins próprios da plataforma, ou seja, para atividades de tratamento que não estão ligadas diretamente ao processo de uso, como condição necessária para ter acesso aos serviços da plataforma. Essa situação é conhecida como *take it or leave it choice*, uma lógica de tudo ou nada, pegar ou largar. Essa prática não é vedada, nem pela GDPR, nem pela LGPD, explicitamente, mesmo que seja possível extrair destas normas uma forte limitação ao seu uso. Isso significa que o fornecedor não pode estabelecer uma lógica de tudo ou nada para uma captura e tratamento indiscriminados de dados pessoais, como condição para o fornecimento dos serviços (a decisão da autoridade antitruste alemã, contra o Facebook, apresentada na Seção 4.2.1, mostra um exemplo de limitação). É preciso delegar ao usuário algum tipo de controle. De todo modo, uma leitura conjunta da GDPR e da Diretiva 2019/770, parece deixar claro a possibilidade de uma oferta onde a remuneração se dá pela cessão de dados pessoais, apesar do esforço retórico da EDPB (2019) em dizer o contrário. Quanto à LGPD, há autores que enxergam no § 3º, do art. 9º, uma abertura para o *take it or leave it*. É o caso de Bruno Miragem (2019):

conforme define o art. 9º, § 3º, da LGPD, ao dispor que “quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.” Trata-se de regra de grande importância nas relações de consumo, sobretudo ao regular as denominadas políticas de tudo

ou nada, (*take-it-or-leave-it-choice*), submetendo o consumidor a opção de aceitar integralmente as disposições ou termos de serviço como condição para sua utilização.

Uma leitura atenta, porém, do referido parágrafo, mostra que não se trata de uma autorização para o *take it or leave it choice*, mas sim uma exigência legal de sobressaltar a informação a respeito dos meios de exercício de direitos quando o tratamento for condição do fornecimento. A condição, por sua vez, pode ser estabelecida contratualmente, sem colocar o consumidor na posição de ceder seus dados pessoais ou não usar a plataforma (*take it or leave it choice*). Em um contexto normativo prospectivo, já considerando a LGPD em vigor, a simples possibilidade de remuneração direta, de serviços digitais, por meio de cessão de dados pessoais não parece ilícita nem uma prática abusiva. O que tem aparência de abusiva é a imposição, pelas plataformas, desse único modelo de pagamento, sem dar ao consumidor a opção de promover o pagamento por outro meio que não envolva a cessão compulsória de uma porção da sua própria personalidade.

A identificação de práticas abusivas pode ser realizada por duas vias paralelas e será configurada se, em qualquer uma delas, ficar evidente o abuso. Na primeira, segue-se a linha do abuso do direito. Na definição de Rizzatto Nunes (2019), trata-se do “resultado do excesso de exercício de um direito, capaz de causar dano a outrem. Ou, em outras palavras, o abuso do direito se caracteriza pelo uso irregular e desviante do direito em seu exercício, por parte do titular”. O próprio Código Civil, no art. 187, traz uma definição do instituto jurídico, associando-o ao ato ilícito, nos seguintes termos, “[t]ambém comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes” (BRASIL, 2002). Resta, agora, desvendar se há abuso do direito por parte das plataformas digitais na definição de seus preços.

De início, é importante lembrar a discussão realizada na Seção 3.1.2.3 que concluiu que, pela própria natureza de seus modelos de negócio, as plataformas podem escolher em que lado carregarão mais o preço a ser pago em dinheiro, do usuário ou do anunciante. Como essa é uma decisão unilateral, colocar todo o pagamento em dinheiro do lado do anunciante é uma escolha natural, pois favorece o efeito de rede e aproveita a vulnerabilidade psicológica do consumidor quando este se encontra frente a uma oferta pretensamente gratuita. Beatriz Kira, ao explicar o modo de precificação das plataformas, detalha o esforço e os custos gerados para manter o peso do pagamento em dinheiro de um único lado e acrescenta que a obtenção dos dados pessoais vai além dos efeitos de rede. A autora utiliza as expressões *multi-homing* e *single-homing* para designar, respectivamente, a utilização de múltiplas plataformas similares, ao mesmo tempo, por um mesmo usuário e o comportamento de fidelidade a uma plataforma única.

Para atrair mais usuários, as plataformas muitas vezes subsidiam os agentes do grupo que são mais sensíveis ao preço ou mais propensos a 'multi-homing'. Quando as plataformas têm que competir por agentes single-homing, os lucros gerados pelo lado multi-homing podem ser transferidos para o lado de single-homing na forma de preços baixos (Armstrong, 2006).

(...)

Nas plataformas da Internet, no entanto, o "custo zero" de muitos dos serviços oferecidos on-line não pode ser explicado apenas em termos de efeitos de redes e subsídios cruzados entre os diferentes lados do mercado. Embora esses incentivos, que são típicos de todos os mercados de plataformas, também sejam verdadeiros nos mercados digitais, eles explicam apenas parcialmente o valor, o tamanho e o poder da maioria das empresas da internet. Na verdade, essas empresas extraem riqueza da coleta e do processamento dos dados pessoais dos usuários, de muitas maneiras diferentes. (KIRA, 2019)

Fica claro, com esse contexto, que há uma artificialidade criada pelas plataformas para capturar mais usuários, maximizar os efeitos de rede e aumentar a captura de dados pessoais. Sobre esse último ponto, o preço zero também reforça o efeito de escala dos dados, externalidade do lado da produção explicado na Seção 3.1.2.2, que não se restringe ao tratamento dos dados exclusivamente captados no processo de uso da plataforma, mas por toda a sua imensa teia de capilaridade física e lógica. Sendo assim, a gratuidade compulsória significa, na prática, um ingresso compulsório em um sistema de vigilância.

O CDC, no inciso IV, do art. 51, considera cláusulas abusivas aquelas que "estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada" (BRASIL, 1990). Marques (2019) salienta que este dispositivo, cumulado com o § 1º do mesmo artigo, cria "verdadeira *norma geral proibitória* de todos os tipos de abusos contratuais" (grifo no original). Neste último dispositivo, configura-se como vantagem exagerada para o fornecedor, dentre outras, aquela que ofende princípios fundamentais do sistema jurídico a que pertence e a que se mostra excessivamente onerosa para o consumidor. Um contrato que, para ser celebrado, exige, como contraprestação, a cessão obrigatória de um direito da personalidade, por si só, é capaz de caracterizar uma violação a Direitos Fundamentais. Além disso, a imposição, pelo fornecedor, de sistema de vigilância ao qual o usuário deve se submeter, sem que lhe seja dada uma opção de uso fora desse sistema, algo que seria perfeitamente possível do ponto de vista técnico, também caracteriza-se como excessivamente onerosa para o consumidor.

Não oferecer ao usuário a possibilidade de se livrar dessa armadilha de extração de dados pessoais, portanto, configura um abuso de direito na definição de preço por parte das plataformas digitais.

A segunda via de análise das práticas abusivas se dá a partir do diálogo com a proteção à concorrência. Como já mencionado, mesmo inexistindo conduta que chame a atenção das autoridades antitruste, o CDC autoriza a intervenção estatal sempre que uma conduta de concorrência desleal ou de abuso de posição dominante puder

infringir dano ou prejuízo aos consumidores. Como base da ordem econômica, cujos contornos são definidos na própria Constituição, a proteção do consumidor deve se dar, também, como mecanismo ativo capaz de aplacar, como ensina José Geraldo Brito Filomeno, “qualquer forma de manobra, ação, acerto de vontades, que vise à eliminação da concorrência, à dominação de mercados e ao aumento arbitrário de lucros” (GRINOVER *et al.*, 2017).

Nesse sentido, a opção pelo preço zero do lado do usuário, como já destacado em diversos pontos, maximiza todas as externalidades positivas presentes no modelo de plataforma. Estes efeitos, juntos, criam uma tendência de concentração e, consequentemente dominação de mercado. O próprio artigo 173, da Constituição Federal, em seu § 4º, estabelece a repressão ao “abuso do poder econômico que vise à dominação dos mercados, à eliminação da concorrência e ao aumento arbitrário dos lucros”, o que se dá, também, pela via do Direito do Consumidor. A própria fixação da remuneração via dados pessoais, sem opção de outra forma de remuneração, por empresas que já possuem uma posição dominante, pode ser considerada ilegal por infringir esse preceito constitucional.

Além disso, o aumento da capacidade de captura de dados pessoais que decorre do próprio modelo de negócio, que impõe, ao consumidor, o fornecimento de dados pessoais como contraprestação à utilização da plataforma, torna mais intenso o efeito de escala de dados, já que ao ingressar, o usuário torna-se exposto a uma imensa teia de captura de dados pessoais. Disponibilizar a opção de pagamento em uma forma diversa aos dados pessoais tem impacto não apenas individual, pelo não ingresso do usuário no sistema de vigilância, mas também coletivo, pois a opção pelo pagamento em dinheiro, por exemplo, para não se submeter ao pagamento por dados pessoais, também contribui para a diminuição do efeito de escala de dados, caso um grande volume de usuários opte por não fornecer seus dados pessoais.

Também se observa, no caso das plataformas, o abuso de posição dominante objetivando o aumento arbitrário dos lucros, que se manifesta de duas formas. Na primeira, a própria escolha arbitrária do preço pecuniário zero, definido pela plataforma, além de maximizar as externalidades, também aproveita a vulnerabilidade psicológica dos consumidores para lidarem com esse tipo de oferta e, principalmente, a vulnerabilidade técnica e informacional, derivada da complexidade que envolve as decisões sobre privacidade e alocação de dados pessoais. Como reflexo dessa combinação de vulnerabilidade informacional com o fato de que os dados pessoais funcionam, nesses contratos, como remuneração direta, há a clara uma violação ao art. 31<sup>52</sup>, do CDC, que exige informação correta sobre o preço.

<sup>52</sup> “A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores.”

Entender os dados pessoais, nas relações de consumo com plataformas digitais, também explicita uma outra violação legal, mais sutil, mas igualmente importante. Ao desconsiderar os dados como parte integrante da remuneração, tem-se a falsa impressão de que todos os usuários pagam o mesmo preço, ou seja, zero. Agora, considerando-os como remuneração, observa-se claramente que cada um, cada indivíduo, paga um preço completamente diferente para usar a plataforma, já que o acervo de dados pessoais utilizado como contrapartida é único e depende de diversos fatores, como tempo de conexão, hábitos de uso e interesses, atraindo com isso, pelo diálogo das fontes, o inciso X<sup>53</sup>, do art. 36, da Lei 12.529/2011, que veda a discriminação de preço. Vale ressaltar que, por si só, a discriminação de preço não é ilegal. A Resolução 20/1999, do CADE (1999), que define discriminação de preços como a situação onde “o produtor utiliza seu poder de mercado para fixar preços diferentes para o mesmo produto/serviço, discriminando entre compradores, individualmente ou em grupos, de forma a se apropriar de parcela do excedente do consumidor e assim elevar seus lucros”, também esclarece que a prática “não é intrinsecamente anticompetitiva, na medida em que, embora aumentando os lucros do produtor, pode não afetar o bem-estar dos consumidores ao não restringir, ou até ao aumentar, o volume de transações no mercado”. Neste ponto, claramente, o CADE refere-se à visão restrita de bem estar do consumidor, ligada exclusivamente a acesso a determinado bem e preço (monetariamente considerado). A partir do conceito mais abrangente de bem estar, que inclui a satisfação dos Direitos Fundamentais, a apropriação, pela plataforma, dos dados pessoais como contraprestação, cria uma situação violadora de direitos pela discriminação de preço. Vale notar que, fixando-se um preço para o uso, o fornecedor mitiga tanto a discriminação de preço, pois cria um parâmetro horizontal de precificação, mesmo que opcional, e também responde adequadamente à violação do artigo 31, do CDC, dando clareza de preço à oferta. Essa discriminação de preço também gera efeitos anticoncorrenciais, tendo em vista que, observados do outro lado da plataforma, são estes dados que geram o efeito de escala de dados, externalidade positiva da qual as plataformas se aproveitam.

A segunda forma de aumento arbitrário dos lucros liga-se à Lei de Metcalfe, tratada na Seção 3.1.2.4, e na progressão não linear do faturamento em relação ao número de usuários. Esse descolamento só ocorre, como já explicitado, devido ao modelo de precificação que leva para zero o valor pago, monetariamente, pelo usuário final, tendo em vista que o pagamento direto, em dinheiro, pelo uso levaria inevitavelmente a um crescimento linear, a partir de um multiplicador do número de usuários, com pequenas variações decorrentes de valores adicionais cobrados por serviços ou conteúdos específicos. Ao basear o modelo de remuneração no outro lado, também

<sup>53</sup> “discriminar adquirentes ou fornecedores de bens ou serviços por meio da fixação diferenciada de preços, ou de condições operacionais de venda ou prestação de serviços;”

reforça os efeitos monopolistas como descrevem Clemons e Madhani (2010)<sup>54</sup>.

Depois de todo esse percurso, desmascarando definitivamente a gratuidade enganosa das plataformas digitais, fica evidente que, tanto pela via do abuso do direito, quanto da proteção à ordem econômica, há prática abusiva realizada pelas plataformas digitais ao determinar, como única forma de contraprestação a remuneração direta por dados pessoais, impedindo o consumidor de estabelecer um outro meio mais adequado, não violador de Direitos Fundamentais: o pagamento em dinheiro.

### 4.3 LIBERDADE PARA PAGAR

Um dos grandes gênios da ciência da computação, John McCarthy foi precursor e cunhou o termo Inteligência Artificial (IA). Fundou, com Marvin Minsky, o Laboratório de Inteligência Artificial do MIT, em 1959. Também criou a linguagem de programação LISP, de importância singular para o desenvolvimento da IA (ISAACSON, 2014). Em LISP, foi criada ELIZA, “um programa que torna possível uma conversa, em linguagem natural, com um computador”, nas palavras de seu criador, Joseph Weizenbaum (1966). Para muitos, ELIZA foi o primeiro programa a passar pelo teste de Turing<sup>55</sup>. McCarthy também previu a oferta de poder computacional como *utility*, tema tratado na Seção 2.1.1. Em 1961, profetizou:

Se os computadores do tipo que eu defendo se tornarem os computadores do futuro, a computação poderá algum dia ser organizada como *utility*, assim como o sistema telefônico é uma *utility*... A computação como *utility* pode se tornar a base de uma nova e importante indústria<sup>56</sup> (GARFINKEL, 1999).

Realmente se tornou. A computação na nuvem, com suas ofertas IaaS e PaaS, e os serviços disponibilizados diretamente pelos donos das infraestruturas (SaaS), operados por empresas com os maiores valores de mercado do mundo, posição que ocupam, em grande medida, por articularem uma quantidade imensa de poder computacional, são uma realidade. A computação defendida por McCarthy, baseada em grande capacidade central de processamento, se caracterizou. Sua visão só não se tornou totalmente hegemônica porque, atualmente, há uma combinação entre grande poder computacional central e terminais inteligentes, diferente do que ele imaginava originalmente, onde os terminais seriam essencialmente meios de promover a entrada e saída de dados.

Em um artigo publicado nos anais da Conferência Internacional O Homem e O Computador, realizada em 1970, McCarthy (2000) descreveu como seria, na sua visão,

<sup>54</sup> Detalhes na Seção 3.1.2.3.

<sup>55</sup> De modo simplificado, uma máquina passa no teste de Turing se em uma conversa, em linguagem natural, entre o programa e um ser humano, um terceiro que observa a conversa não consegue distinguir quem é o humano e quem é a máquina.

<sup>56</sup> No original: “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility... The computer utility could become the basis of a new and important industry.” (tradução livre)



a vida onde as pessoas tivessem, em casa, um terminal de informação (*home information terminal*) que, conectado pelo sistema de telefonia a um computador de tempo compartilhado, poderia “acessar arquivos contendo todos os livros, revistas, jornais, catálogos, horários de vôo, muitas outras informações públicas não disponíveis à época e vários arquivos pessoais”<sup>57</sup>. Nestes terminais, além de ter acesso aos conteúdos, seria possível fazer operações de compra e venda, realizar comunicações com outras pessoas ou organizações e fazer processamento de informações de diversas formas. As previsões são impressionantes, principalmente ao se considerar que foram feitas mais de vinte anos antes do início da internet comercial e um ano antes do lançamento do primeiro chip Intel.

Nesse mesmo artigo, ao falar sobre acesso a conteúdo, previu algo que ainda não se concretizou:

A publicidade no sentido de algo que pode forçar a atenção de um leitor desaparecerá porque será muito fácil ler através de um programa que oculte material indesejável. No entanto, as pessoas ainda querem saber o que está à venda e ainda querem ver a história dos vendedores sobre por que elas deveriam comprar seus produtos. Provavelmente, a Life ainda poderá receber dinheiro dos anunciantes; muitas pessoas ainda querem saber o que é anunciado na Life, mas quem não quer saber poderá evitá-lo automaticamente<sup>58</sup> (MCCARTHY, 2000).

Cinquenta anos depois, cada pessoa interage com diversos equipamentos, que ocupam a posição de terminal, para acesso a conteúdos e serviços disponibilizados a partir de grandes estruturas computacionais. Alguns deles seguem o indivíduo por onde ele vai. Outros são vestíveis e, portanto, estão ligados ao corpo. A partir deles, praticamente todas as ações (e também não ações) do usuário são monitoradas. E a publicidade nunca esteve tão presente, de forma tão próxima. Agora, além da captura do tempo, para que se tenha acesso a esse mundo de conteúdos e serviços, é necessário fornecer dados pessoais, que transformam os usuários em alvos adequados e precisos, sendo a oportunidade de abatê-los vendida na forma de publicidade comportamental. Assim como McCarthy não previu a força dos terminais inteligentes, também não imaginou que, meio século depois, as pessoas passariam a viver soterradas por publicidade inteligente, que traz consigo a sombra da ameaça de uma sociedade da vigilância.

<sup>57</sup> No original: “has access to files containing all books, magazines, newspapers, catalogs, airline schedules, much additional public information not now kept, and various files personal to the user.” (tradução livre)

<sup>58</sup> No original: “Advertising in the sense of something that can force itself on the attention of a reader will disappear because it will be too easy to read via a program that screens out undesirable material. However, people will still want to know what is for sale and will still want to see the seller’s story about why they should buy it. Probably, Life will still be able to get money from advertisers; many people will still want to know what is advertised in Life, but those who do not want to know will be able to avoid it automatically.” (tradução livre)

Neste capítulo, em grande medida, resgata-se a ideia de John McCarthy. Mas hoje, infelizmente, ter a opção de decidir se deseja ou não ser alvo de publicidade, barrando-a na ponta do consumidor, já não é mais suficiente. Trazido para os dias atuais, é necessário pensar mecanismos, jurídicos e tecnológicos, capazes de tornar eficaz o poder de escolha, das pessoas, em como alocar seus dados pessoais. E isso, como tudo no mercado, tem um preço, que precisa ser claro e justo.

Nas próximas seções, será apresentada uma sugestão de regulação para plataformas digitais que se concentra na ideia de que os valores envolvidos nas contratações de serviços digitais devem ser explicitados, em dinheiro. Não significa o fim da oferta remunerada diretamente por dados pessoais, mas abre espaço para que as pessoas tenham uma outra opção, acabando com o caráter compulsório da cessão de dados pessoais como contrapartida pelo uso destes serviços.

### 4.3.1 Definindo os alvos da regulação

O primeiro desafio que se impõe ao se estruturar uma proposta de regulação está relacionado à definição de qual ou quais segmentos de mercado serão atingidos. Em um ambiente tão complexo quanto o dos negócios digitais, muitas vezes organizados como mercados de dois ou múltiplos lados, essa delimitação pode ser feita a partir da adoção de diversos parâmetros.

Orla Lynskey (2019), em uma sugestão de regulação a partir da imposição de uma responsabilidade especial a um grupo específico de empresas, utilizando, por analogia, o conceito de responsabilidade especial<sup>59</sup> imposta pela lei antitruste a companhias em posição dominante, aponta como alvo as empresas que detêm o que ela chamou de “data power”, que foi assim definido:

O *data power* é uma forma multifacetada de poder disponível para plataformas digitais, decorrente de seu controle sobre os fluxos de dados. Como as plataformas on-line agem como uma interface entre seus vários clientes (provedores de conteúdo, anunciantes, usuários individuais etc.), elas estão em uma posição única para controlar o fluxo de informações entre os participantes no ecossistema digital e coletar dados sobre as ações de cada uma dessas partes na esfera digital<sup>60</sup> (LYNSKEY, 2019b).

<sup>59</sup> Na dicção do Tribunal de Justiça da União Europeia (2007), “embora a conclusão de que uma empresa está em posição dominante não constitua, em si mesma, nenhuma censura a essa empresa, incumbe, no entanto, a esta última, independentemente das causas dessa posição, a responsabilidade especial de não impedir, através do seu comportamento, uma concorrência efectiva e não falseada no mercado comum”. Em um contraponto com os mercados tradicionais, Beatriz Kira (2019) reforça que empresas com posição dominante, que atuam em mercados digitais, podem utilizar o grande volume de dados que têm a disposição para realizar condutas anticompetitivas, o que cria uma responsabilidade especial de não abusar de sua posição para restringir a concorrência.

<sup>60</sup> No original: “Data power is a multifaceted form of power available to digital platforms, arising from their control over data flows. As online platforms act as an interface between their various constituents (content providers, advertisers, individual users, etc.), they are in a unique position to control the flow of information between participants in the digital ecosystem, and to gather data about the actions of each of these parties in the digital sphere.” (tradução livre)

Essa posição de *gatekeeper*, bem como os termos *plataform power* e *digital dominance*, estão bem documentados e têm recebido atenção acadêmica, confirma a autora, indicando que os consideram excessivamente amplos. Também faz uma crítica mais pontual quanto ao uso da expressão *plataform power*, pois plataforma, isoladamente considerada, tende a incluir todas as estruturas de dois ou múltiplos lados, enquanto *plataform power* não consegue expressar, com clareza, qual problema se está enfrentando. Ao contrário de *data power* que, segundo ela, indica que o poder se localiza exatamente no controle sobre os dados e esse é o problema regulatório que se quer resolver. Além disso, nem toda plataforma possui *data power*, pois para tanto é necessário concentrar grande volume e variedade de dados (LYNSKEY, 2019b).

A EDPB (2018), em declaração sobre concentração econômica, alertou que a privacidade e a proteção de dados são relevantes para a avaliação de potenciais abusos de posição dominante, bem como em fusões de empresas, sempre que as circunstâncias envolvam ou que possam acarretar significativo *informational power*, em sentido muito equivalente ao utilizado por Lynskey com a expressão *data power*.

Apesar de interessante, a delimitação de Lynskey também enfrenta problemas de amplitude relevantes. Primeiro, porque a análise de volume e variedade de dados é difícil de ser feita, principalmente ao se fugir do âmbito das Big Techs. Como medir se a quantidade e a qualidade dos dados tratados é suficiente para caracterizar “data power”? Uma das características de uma boa regulação é deixar o menor número possível de dúvidas sobre sua aplicabilidade e, a não ser que exista uma classificação prévia, feita por uma autoridade competente, é difícil imaginar um critério objetivo para esse enquadramento. Empresas como Uber e AirBnB, que operam, atualmente em mercados específicos, possuem dados de variedades suficientemente diferentes para os enquadrarem como empresas subordinadas à nova legislação? Trazendo a ideia para o contexto brasileiro, as Organizações Globo, com sua estratégia de digitalização dos negócios de mídia, seria detentora de *data power*? Outra questão é igualmente importante: seria possível estabelecer obrigações horizontais para os diferentes modelos de negócio potencialmente geradores de *data power*? A Amazon, por exemplo, tem um modelo de negócio com presença evidente de “data power”. A nova regulação aplicável a Google e Facebook, seria eficaz para a Amazon? Uma das sugestões dadas por Lynskey seria o enquadramento das empresas que possuem “data power” como empresas que prestam serviços públicos (2019). Essa seria uma alternativa viável, por exemplo, para a Amazon?

Estas questões são muito difíceis de serem enfrentadas na prática. Principalmente quando é necessário estabelecer critérios objetivos, que tornem a regulação efetivamente aplicável. Neste sentido, levando em consideração a aplicabilidade, a sugestão proposta neste trabalho atingiria: toda plataforma em que o cliente de um dos lados compre acesso a alguém de outro lado, por meio de publicidade.

Este contorno, mais amplo do que o de plataformas digitais que disponibilizam seus serviços sem contrapartida monetária por parte do usuário final, é necessário para que não se abra a possibilidade para a disponibilização de serviços *premium*, com baixo custo para o usuário, simplesmente como forma de fugir da regulação. As implicações desse escopo de aplicabilidade ficarão mais claras na Seção 4.3.2.2. Assim, serviços como os disponibilizados por Google, Facebook, Twitter etc, se encaixam no conceito, mas outros como Spotify e Globoplay, bem como os veículos de mídia que, eventualmente, mantenham suas estruturas de gestão de anúncios também se enquadrariam. Esse tema específico, dos veículos de mídia, será tratado com detalhes, incluindo um exemplo, na Seção 4.3.2.1.

### 4.3.2 No mercado, tudo tem um preço

Bert-Jaap Koops, professor da escola de Direito da Tilburg University, faz um paralelo interessante entre os dados e a luz, que hora se comporta como partícula, hora como onda. Na sua visão, os dados ora podem ser pessoais, ora são não pessoais, dependendo do contexto, o que, de certa forma faz sentido, já que a caracterização do dado pessoal é contextual, como abordado na Seção 4.1.2.

Para aplacar a estranheza de algo que se comporta de duas maneiras, muito influenciada pelas percepções sensoriais macroscópicas às quais estamos submetidos, Niels Bohr<sup>61</sup>, um dos pais da física quântica, formulou o *Princípio da Complementariedade*, que pode ser enunciado da seguinte maneira:

Os aspectos ondulatórios e corpuscular de uma entidade quântica são ambos necessários para uma descrição completa. No entanto, ambos os aspectos não podem ser revelados simultaneamente numa mesma experiência. O aspecto que irá se revelar, numa certa experiência, está determinado pela natureza da própria experiência (HALLIDAY; RESNICK; WALKER, 1995).

Bohr esclarece, com seu princípio, que dependendo da forma como se interage com a luz, ela deverá ser interpretada como partícula ou como onda, mas em nenhuma experiência será possível interpretá-la simultaneamente como onda e como partícula.

Praticamente todo esse trabalho é construído sobre a ideia de um caráter duplo dos dados pessoais, que ora devem ser vistos como pequenas peças que formam o mosaico informacional da personalidade, ou seja, são observadas como partículas, ora devem ser enxergadas como bens economicamente apreciáveis, que podem - e são - processados para fins econômicos, onde o ponto central de preocupação é a manutenção do fluxo de dados, que pode ser associado, na metáfora da luz, com um comportamento de onda. Nessa segunda visão, o dado pessoal individualmente

<sup>61</sup> Niels Henrik David Bohr, vencedor do Prêmio Nobel de Física, em 1922, “por seu trabalho na pesquisa da estrutura dos átomos e da radiação emitida por eles” (NOBELPRIZE.ORG, 2020). No original: “for his services in the investigation of the structure of atoms and of the radiation emanating from them.”(tradução livre)

considerado perde relevância (para esse observador) frente à importância do volume agregado de dados. Assim, por este prisma, a melhor forma de abordar os dados pessoais é como commodities.

Há uma grande controvérsia no entendimento dos dados pessoais como commodities, como se essa conclusão fosse o reconhecimento de que o sujeito se transformou definitivamente em objeto lançado e vendido ao mercado. Mas essa estranheza se dá pelo fato de se espelhar um comportamento adequado para a observação a partir de uma perspectiva quando se visualiza o problema por outra. Václav Janeček e Gianclaudio Malgieri (2019), fazem uma boa ponderação sobre esta questão que vale ser considerada:

a análise de dados pessoais como *res extra commercium* é problemática: sua natureza como mercadoria (in)alienável pode parecer ambígua em muitos marcos legais. No entanto, independentemente das definições e pronunciamentos nos documentos legais, se focarmos apenas na possibilidade de processar dados pessoais com base na monetização (o controlador de dados requisita o uso ao titular dos dados pessoais em troca de dinheiro ou por um serviço valioso, ou o controlador de dados troca dados pessoais com um terceiros, por exemplo, uma empresa, em troca de dinheiro), concluímos que há uma regra limitada de alienabilidade<sup>62</sup>

É exatamente isso que acontece na vida real. É a essa realidade que a Diretiva 2019/770, da União Europeia, dá contornos jurídicos, tentando se esquivar das “definições e pronunciamentos legais” que rechaçam a comercialização ou a comoditização dos dados pessoais. Nessa linha, também, se posiciona a autoridade antitruste alemã, por via reversa, ao considerar a existência de um conjunto de dados pessoais que pode ser processado pela plataforma, baseado no legítimo interesse, como contrapartida pela não remuneração direta, em dinheiro, dos serviços.

Agrega-se a esse problema o fato de que legislações como a GDPR - e a LGPD -, criam um regime de proteção centrado no indivíduo, com ênfase em mecanismos de controle individual sobre os dados pessoais (LYNSKEY, 2019b). Mesmo os padrões de *enforcement* são calcados na avaliação e no impacto do tratamento de dados, sob a ótica do titular. Essa característica das legislações específicas de proteção de dados pessoais está bem alinhada à sua finalidade específica, mas pode não ser suficiente, como se sustentou na Seção 4.1.

O correto enquadramento da perspectiva dos dados como commodities pode - e deve - ajudar a garantir um nível mais alto de proteção dos dados pessoais individualmente considerados, ou seja, vistos sob a ótica do indivíduo. Negar a realidade dos

<sup>62</sup> No original: “the analysis of personal data as *res extra commercium* is problematic: their nature as an (in)alienable commodity might appear ambiguous in many legal frameworks. However, regardless of definitions and pronouncements in legal documents, if we focus just on the possibility of processing personal data on a monetization basis (either the data controller asks the data subject for personal data in exchange for money or for a valuable service, or the data controller exchanges personal data with a third recipient, e.g. a business, in exchange for money), we conclude that there is a limited alienability rule.” (tradução livre)

dados pessoais como commodities elimina, portanto, uma grande gama de possibilidades de regulação que podem ser utilizadas para aumento da eficácia dos Direitos da Personalidade. É para essa ótica que a sugestão de regulação se volta. Observar o volume agregado de dados, que cria vulnerabilidades perigosas aos indivíduos e é efetivamente operado como commodity, e buscar enxergar mecanismos capazes de aumentar a eficácia dos Direitos Fundamentais. Para isso, é preciso enfrentar o tema da precificação dos dados pessoais para, em seguida, partir para os contornos da regulação.

#### 4.3.2.1 Precificação indireta dos dados pessoais

Muitas discussões que envolvem a observação dos dados pessoais como bens economicamente apreciáveis acabam por desaguar nas questões da precificação que abordam os dados como se fossem bens rivais, tratando o tema a partir de uma visão baseada em propriedade e posse. Nesse sentido, Pentland (2013) faz uma analogia entre as plataformas digitais e os bancos.

*A chave para o New Deal é tratar os dados pessoais como um ativo.(...)*

Você tem o direito de possuir os dados que lhe digam respeito. Independente de qual entidade realizou a coleta, os dados pertencem a você e você pode acessar os dados a qualquer momento. Os responsáveis pela coleta de dados, portanto, desempenham um papel semelhante a um banco, gerenciando os dados em nome de seus “clientes”. Você tem o direito de ter o controle completo de seus dados. Os termos de uso devem ter opt-in [aceite expresso] e devem ser claramente explicados em linguagem simples. Se você não estiver contente com a forma como a empresa usa seus dados, você pode remover todos eles, assim como você fecha uma conta em um banco que não oferece serviços satisfatórios.

Você tem o direito de dispor ou distribuir seus dados. Você tem a opção de querer destruir seus dados ou redistribuí-los.<sup>63</sup>

Como já se pode constatar, pela análise realizada na Seção 3.2.1.1, os dados pessoais são não rivais e os atributos de propriedade não se encaixam integralmente a bens com as características peculiares dos dados. Além disso, pensar o comércio de dados pessoais, em um mercado aberto cria um grande inconveniente prático: impõe a cada pessoa uma tarefa de gestão de seu acervo de dados pessoais, de forma similar à maneira com que administra suas receitas em instituições financeiras. Essa dificuldade de apreciação do valor monetário dos dados acontece, essencialmente,

<sup>63</sup> No original: “The key to the New Deal is to treat personal data as an asset. (...) You have the right to possess data about you. Regardless of what entity collects the data, the data belong to you, and you can access the data at any time. Data collectors thus play a role akin to a bank, managing the data on behalf of their “customers.” You have the right to full control over the use of your data. The terms of use must be opt-in and clearly explained in plain language. If you are not happy with the way a company uses your data, you can remove those data, just as you would close your account with a bank that is not providing satisfactory service. You have the right to dispose of or distribute your data. You have the option to have data about you destroyed or redeployed.” (tradução livre)

porque os parâmetros de avaliação levam em consideração os dados individualizados, na perspectiva do indivíduo que faz a cessão. Uma outra perspectiva, mais adequada à visão dos dados pessoais como commodities, pode ajudar a criar mecanismos mais eficientes de controle e de proteção.

Plataformas digitais, pelas suas próprias características, raramente colocam em comércio os dados *in natura*. E existem três bons motivos para isso: primeiro, porque informação que pode ser genericamente obtida (como o conteúdo de páginas dispersas pela web, no caso das buscas) tem preço de venda igual ao seu custo marginal, ou seja, zero (SHAPIRO; VARIAN, 1999); segundo porque dados obtidos diretamente pelas plataformas, possuem um valor que elas não desejam compartilhar e terceiro porque é mais lucrativo se posicionar como conector de diversas pontas (*gatekeeper*) e aproveitar todas as externalidades positivas geradas por este modelo. Assim, considerar o dados em comércio significa entender como os dados funcionam como matéria-prima, consumida em um processo de produção, e não como bens com diversos ciclos de circulação. A abordagem de Cohen (2019), apresentada na Seção 2.2.2, mostra a força desse modelo de negócio, que captura o dado como uma matéria-prima livre para ser explorada e que, nos domínios da plataforma, é tratada como um bem privado.

Partindo do pressuposto de que os dados pessoais são uma matéria-prima para uma outra relação contratual entre a plataforma e o anunciante e, também, que o serviço oferecido pela plataforma ao usuário final poderia ser disponibilizado por uma relação contratual direta, em que o usuário final pagaria pelo serviço disponibilizado pela plataforma, sem a existência da transação publicitária, que consome dados pessoais e atenção do usuário, pode-se considerar a diferença entre o preço pago em uma hipotética contratação direta, ou seja, sem apropriação de dados pessoais e atenção<sup>64</sup>, e o preço pago na contratação onde há essa apropriação, como o valor agregado pelos dados pessoais ao negócio da plataforma.

Esse valor será designado, daqui por diante, de **valor-dados por usuário**.

Um exemplo real ajuda a deixar claro esse conceito. Após a entrada em vigor da GDPR, o jornal The Washington Post reformulou seu modelo de cobrança para a Europa, disponibilizando três opções para os usuários: na primeira, gratuita (oferta *Free*), que dá direito à leitura de um número limitado de artigos por mês, o usuário deve consentir com o uso de *cookies* e outros mecanismos de rastreamento para publicidade personalizada, ou seja, marketing comportamental (*behavior marketing*). Na segunda opção, o usuário paga 60 euros por ano para ter acesso ilimitado ao site do veículo e também aos seus aplicativos, mas, da mesma forma como acontece com o uso gratuito, deve consentir com o rastreamento e uso de dados pessoais para publicidade

<sup>64</sup> Assim como na elaboração realizada na Seção 4.2.2.1, aqui também considera-se a atenção com um aspecto de valor residual, concentrando-se a carga valorativa nos dados pessoais.

personalizada (oferta *All-Access Digital*). Na terceira oferta, paga-se 90 euros por ano para ter acesso irrestrito a conteúdo e aplicações, mas nesse caso não há exibição de anúncios nem rastreamento de dados para fins de publicidade direcionada (oferta *Premium EU Ad-Free*). A imagem da Figura 6 reproduz a página da oferta.

Figura 6 – The Washington Post: página de assinatura para a Europa

The Washington Post  
Democracy Dies in Darkness

Are you a subscriber? [Sign in here](#)

## Support great journalism.

We rely on readers like you to uphold a free press.

Free	All-Access Digital	Premium EU Ad-Free
<b>Browse now</b>	<b>Subscribe now</b>	<b>Subscribe now</b>
<ul style="list-style-type: none"> <li>✓ Read a limited number of articles each month</li> <li>✓ You consent to the use of cookies and tracking by us and third parties to provide you with personalized ads</li> </ul>	<ul style="list-style-type: none"> <li>✓ Unlimited access to washingtonpost.com on any device</li> <li>✓ Unlimited access to all Washington Post apps</li> <li>✓ You consent to the use of cookies and tracking by us and third parties to provide you with personalized ads</li> </ul>	<ul style="list-style-type: none"> <li>✓ Unlimited access to washingtonpost.com on any device</li> <li>✓ Unlimited access to all Washington Post apps</li> <li>✓ <b>No on-site advertising or third-party ad tracking</b></li> </ul>

Fonte: Disponível em: <https://www.washingtonpost.com/gdpr-consent/>. Acesso em 10/02/2020.

Os críticos desse modelo alegam que o jornal está forçando a compra de um Direito Fundamental, e tratando os dados pessoais como mercadoria. Essa seria a ótica apropriada para uma abordagem realizada a partir do ponto de vista do usuário final, mas que não se encaixa ao se observar o problema sob o prisma do uso dos dados pessoais do outro lado da plataforma. Retomando uma conclusão da Seção 4.2.2.1, na relação de remuneração direta por meio de dados pessoais, o valor pago por cada usuário é único e está ligado a diversas características do próprio usuário e de seus hábitos. Portanto, em uma oferta como esta, The Washington Post não precifica os dados de cada usuário, mas sim projeta uma estimativa do valor agregado dos dados ao modelo de negócio.

Numa projeção perfeita, a receita aferida em um cenário onde todos os usuários optam pela oferta *All-Access Digital* deveria ser igual à receita aferida quando todos os usuários optam pela oferta *Premium EU Ad-Free*. Assim, a diferença do valor obtido



pelo pagamento direto entre os dois extremos seria o equivalente ao valor agregado pelos dados pessoais mais a atenção do usuário. Considerando esse modelo ideal, onde o dono da plataforma tenta estabelecer um valor justo pelo agregado de todos os dados pessoais e toda atenção dos usuários, o que se reflete no preço final é simplesmente a divisão entre esse valor agregado, que daqui em diante chamaremos simplesmente de **valor-dados**, por uma quantidade estimada de usuários.

Utilizando o Facebook como exemplo, a empresa fechou o ano com um faturamento gerado por publicidade de US\$ 69,655 bilhões e 2,5 bilhões de usuários únicos que utilizaram a plataforma pelo menos uma vez por mês. Neste sentido, um valor-dados por usuário equilibrado, considerando a margem operacional de 34% e o resultado líquido de US\$ 18,485 bilhões, equivalente a 26,54% do faturamento, poderia ser o resultado da divisão entre o faturamento gerado por publicidade e o número de usuários únicos mensais, que daria um valor próximo a US\$ 28,00 dólares anuais (FACEBOOK, 2020).

Importante sempre ter em mente que o valor-dados por usuário é um parâmetro para definição de preço, não exclusivo, já que a oferta sem remuneração em dinheiro ainda pode existir, para o serviço onde nem os dados pessoais, nem a atenção do usuário sejam utilizados para oferta de publicidade. Na prática, trata-se de um valor arbitrário a ser definido pelo dono da plataforma.

É preciso considerar, portanto, que sempre há a possibilidade de manipulação desse valor pelo fornecedor. As plataformas aproveitam os efeitos de rede que, em grande medida, não estariam presentes caso a remuneração ocorresse de forma direta. Isso poderia levar o dono da plataforma a estabelecer um valor-dados por usuário exorbitante, com o objetivo de desestimulá-los a optarem pela oferta paga diretamente. Voltando ao caso do Facebook, o valor-dados por usuário poderia ser fixado em, por exemplo, US\$ 600,00 dólares anuais (US\$ 50,00 mensais), o que inviabilizaria a oferta.

Uma boa maneira de desarmar esse desequilíbrio na fixação arbitrária do preço, seria estabelecer um imposto sobre o valor-dados, a ser pago pelo dono da plataforma, em uma adaptação da ideia original de Arnold Harberger, nominada por Eric Posner e Glen Weyl (2019) de imposto autoavaliado sobre a propriedade comum (*common ownership self-assessed tax*), pensado para imóveis, onde cada proprietário seria obrigado a declarar o valor da sua propriedade, que seria tornado público, sendo o proprietário também obrigado a vender a propriedade caso um comprador oferecesse o preço declarado. Sobre o valor declarado também incidiria o imposto. É necessário deixar claro que a fixação de um preço, como o valor-dados por usuário, é uma adaptação, para os dados, do modelo inicialmente pensado por Harberger para os imóveis.

Retornando para o exemplo do Facebook, ao fixar, hipoteticamente, o valor-dados por usuário, em US\$ 28,00 por ano, a base de cálculo do imposto, equivalente

ao valor-dados, seria US\$ 70 bilhões de dólares, enquanto para uma fixação de US\$ 600 por ano, a base de cálculo saltaria para US\$ 1,5 trilhão. Essa diferença tende a desestimular preços arbitrários para disponibilização dos serviços sem uso dos dados pessoais ou da atenção dos usuários para disponibilização de publicidade. Valores muito baixos diminuiriam o valor do imposto, mas também estimularia os usuários a optarem pela versão paga, preservando seus dados pessoais, sem causar restrição de uso da plataforma. Novos concorrentes poderiam utilizar estratégias de preço mais baixo, adotando uma postura de maior preocupação com a privacidade e a proteção de dados dos usuários sem fechar as portas, totalmente, para os usuários que desejam utilizar a plataforma gratuitamente. Por uma postura menos dependente de dados pessoais, essas empresas seriam premiadas com impostos mais baixos.

Finalizada a modelagem da precificação dos serviços a partir do valor-dados por usuário, é preciso aumentar o nível de detalhamento da vedação à gratuidade compulsória.

#### 4.3.2.2 Os contornos da vedação à gratuidade compulsória

A ideia de uma opção, disponibilizada pelas plataformas, onde o usuário possa pagar diretamente pelos serviços, sem que seus dados pessoais fossem usados para finalidades próprias do fornecedor, não é nem original, nem nova. Na visão de Pasquale (2013):

Se as plataformas no coração da economia digital estivessem totalmente comprometidas com monetização e eficiência, elas ofereceriam aos consumidores mais opções. Um usuário poderia ter a oportunidade de pagar, digamos, duas vezes o valor presente líquido dos dados que ele esperaria gerar para a plataforma. Em troca, ele teria certeza de que seus dados não estariam disponíveis para o uso da plataforma. Mas esse arranjo aparentemente ótimo de Pareto não é oferecido, e sua invisibilidade sugere porque os desequilíbrios de poder, em vez de eficiência ou consentimento, devem ser o foco normativo das leis antitruste e de privacidade<sup>65</sup>.

Apesar de ser uma percepção de capacidade, ou vontade, de pagamento difícil de ser aferida, assim como também não é fácil calcular o valor presente dos resultados futuros gerados a partir do tratamento dos dados pessoais, Pasquale faz uma leitura bastante correta sobre a viabilidade de existência de uma oferta que não envolva o tratamento dos dados pessoais para fins próprios das plataformas; entre a falta de interesse desses *players* em implementarem esta opção, certamente porque deformaria, em alguma medida, um modelo onde aproveitam externalidades que favorecem

<sup>65</sup> No original: "If the platforms at the heart of the digital economy were entirely committed to monetization and efficiency, they would offer consumers more options. A user might be offered the opportunity to pay, say, twice the discounted present value of the data he was expected to generate for the platform. In return, he is assured that his data is unavailable for the platform's use. But such a seemingly Pareto-optimal arrangement is not on offer, and its invisibility suggests why imbalances in power, rather than efficiency or consent, ought to be the normative focus of antitrust and privacy law." (tradução livre)

a fixação de posições dominantes e, em alguns casos, de monopólios ou oligopólios e, também, sobre o alinhamento, em grande medida, dos modelos de negócio das plataformas, com aproveitamento econômico dos dados pessoais, e as legislações implementadas para proteger esses mesmos dados pessoais.

Já Malgieri e Custers (2018) sugerem uma abordagem diferente. Ao invés de estabelecer a vedação à gratuidade compulsória, ou seja, a existência de uma opção de oferta que não utilize os dados pessoais nem a atenção dos usuários como contrapartida pela utilização da plataforma, apresentam a ideia de um novo dever de informação, por parte do controlador, que poderia ser incluído no rol de obrigações do art. 13, da GDPR, forçando a plataforma a informar, baseado em parâmetros objetivos, o valor dos dados pessoais relevantes para a transação econômica. No próprio paper, esclarecem ser muito difícil definir o valor a ser apresentado para o titular dos dados. O mais interessante, porém, é que a sugestão de um dever de informação derivou do fato dos autores considerarem que uma oferta que veda o uso dos dados pessoais para fins próprios da plataforma, colocada ao usuário como uma opção frente a outra oferta que faz esse tipo de uso, possibilitando uma escolha ativa do titular, seria incompatível com a GDPR:

estes modelos de escolha ativa não são compatíveis com a nova legislação da UE em matéria de proteção de dados (regulamento geral sobre proteção de dados). O Artigo 7 (4)<sup>66</sup> estabelece que, ao avaliar se o consentimento é concedido livremente, será levado em consideração se, entre outros aspectos, a execução de um contrato, incluindo a prestação de um serviço, depende do consentimento no tratamento de dados pessoais que não é necessário para a execução desse contrato.<sup>67</sup>

Levando o Artigo 7 (4) em consideração, mesmo nos serviços oferecidos atualmente, pelas plataformas, não há consentimento livre na utilização dos dados, para fins próprios da plataforma ou de terceiros, como contrapartida pelo seu uso. O indivíduo é obrigado a aceitar ou não utilizar, verdadeiro ‘take-it-or-leave-it-choice’. Mesmo assim, esses serviços continuam sendo oferecidos legalmente na União Europeia. Isso se dá porque a base legal que dá sustentação a essas atividades de tratamento não é o consentimento, mas sim o legítimo interesse do controlador ou de terceiros, que encontra respaldo na legítima expectativa do usuário que utiliza a plataforma sem precisar desembolsar um montante financeiro. A abrangência desse uso deve, portanto, passar pelo teste de proporcionalidade, de forma que não haja uma extrapolação, por parte do

<sup>66</sup> Texto do dispositivo legal, na versão em português, da GDPR: “Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.”

<sup>67</sup> No original: “these active choice models are not compatible with the new EU data protection legislation (the General Data Protection Regulation). Article 7(4) states that when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” (tradução livre)

controlador, no uso dos dados de seus usuários para finalidades muito exóticas às suas expectativas razoáveis e, também, que não haja tratamento de um volume de dados que ultrapasse os limites do razoável. Essa foi a leitura, em linhas gerais, estabelecida pela autoridade antitruste da Alemanha, no caso do Facebook envolvendo a utilização de dados captados por outras aplicações de sua propriedade e, também, de sites ou aplicações de terceiros. A autoridade, com razão, concluiu que os dados captados fora dos limites da rede social não estavam abarcados no legítimo interesse que sustenta o uso dos dados como contrapartida pela disponibilização da plataforma. Assim, há a necessidade de consentimento e, no caso específico, a autoridade entendeu, também acertadamente, que o consentimento, na forma apresentada nos termos de uso, não eram compatíveis com as exigências da GDPR.

Portanto, partindo-se desse entendimento, é possível dentro do escopo normativo tanto da GDPR quanto da LGPD, uma oferta que não envolva dados pessoais e atenção como contraprestação pela disponibilização da plataforma, mesmo porque não se trata de estabelecer um preço pelos dados pessoais individualmente considerados, de um usuário específico, mas de uma medida do valor total dos dados (valor-dados), dividido pelo número de usuário (valor-dados por usuário), utilizado como parâmetro de precificação. Portanto, como visto na seção anterior, os dados pessoais, quando observados pela perspectiva de seu uso em volume, para disponibilização e para aumento de eficiência de serviços digitais, têm características de commodities. Esses dados pessoais, por sua vez, são obtidos como remuneração direta realizada pelos usuários em contrapartida pela utilização dos serviços. Além dos dados, esse processo captura a atenção (uma perspectiva do tempo) dos usuários, que também é comoditizada (GRIMMELMANN, 2018).

Traçado esse contexto, a regulação sugerida cria uma obrigação para toda plataforma em que o cliente de um dos lados compre acesso a alguém de outro lado, por meio de publicidade (*players* atingidos pela regulação), de estabelecer uma oferta, não necessariamente exclusiva, que atenda três requisitos:

- a.** não utilize dados pessoais com base no legítimo interesse do controlador ou de terceiros.
- b.** não apresente anúncios;
- c.** não tenha preço zero.

O caráter amplo dos três requisitos exigidos para a oferta obrigatória gera impactos substanciais nos modelos de negócio das plataformas. A não utilização de dados pessoais com base no legítimo interesse, por exemplo, veda diretamente a utilização dos dados pessoais, coletados no próprio uso da plataforma, para fins de perfilização e, também, deixa clara a vedação da consolidação de dados originados fora das

fronteiras da aplicação, nos moldes do que decidiu a autoridade antitruste alemã, no caso Facebook, a não ser que exista uma outra base legal - no caso específico, o consentimento livre - que a avalize. Outro impacto bastante relevante diz respeito ao uso de dados pessoais, de modo consolidado, para oferecimento de ferramentas de gestão de presença digital e performance de marketing para outras empresas, caso do Google Analytics, por exemplo. Mesmo que os dados sejam apresentados de modo agregado, sem identificação do titular para o usuário da aplicação, na origem tratava-se de um dado pessoal, muitos, inclusive, capturados nas próprias páginas das empresas usuárias da plataforma de análise, a partir da inserção de pedaços de código criados pelo dono da plataforma, especificamente para capturar esses dados. A interrupção do tratamento de dados pessoais com base no legítimo interesse pode gerar um grande impacto na eficácia dos mecanismos de capilaridade física e lógica montados pelas plataformas para captura de dados pessoais. Além disso, impacta no efeito de escala de dados, já que quanto mais usuários aderirem ao modelo pago, menor será o volume de dados disponíveis para perfilização e segmentação de usuários. O pagamento direto também tende a diminuir o deslocamento das curvas de crescimento do número de usuários e crescimento do faturamento, como no caso do Facebook, com curva de faturamento apresentando crescimento quadrático<sup>68</sup>. Quanto mais usuários optarem pelo modelo de pagamento direto em dinheiro, mais linear se tornará a curva de crescimento, também aplacando o efeito de rede observado no faturamento.

Já o impedimento da apresentação de anúncios tende a gerar um impacto expressivo nos efeitos de rede indiretos, já que, para os anunciantes, um grande volume de usuários que não podem visualizar anúncios é irrelevante. Mas há um outro aspecto também expressivo, que envolve plataformas de distribuição de anúncios, como o Google AdSense. A vedação de apresentação de anúncios não deve se restringir apenas aos espaços publicitários operados dentro dos sites e aplicações do próprio dono da plataforma, mas deve atingir todos os anúncios gerenciados por este dono de plataforma. A restrição de apresentação de anúncios atinge os efeitos indiretos de rede do lado dos *publishers* que utilizam as plataformas de distribuição de anúncios, já que não há nenhum incentivo, para o veículo, na adoção de uma plataforma que não possa apresentar os anúncios para uma parte expressiva das pessoas que visitam a versão digital do veículo ou a página de uma empresa ou pessoa que utiliza a rede de anúncios para a monetização de seu negócio ou atividade.

O último fator é a própria vedação à gratuidade monetária compulsória. Tem como principal objetivo obrigar o fornecedor a explicitar o valor, a partir da sua avaliação, dos dados pessoais agregados (dados pessoais como commodities). Também tem, como objetivo secundário, a criação de parâmetros mais claros para que o indivíduo possa tomar uma decisão consciente sobre a cessão ou não dos seus dados

<sup>68</sup> Mais detalhes podem ser obtidos na Seção 3.1.2.4

peçoais como contrapartida à utilização dos serviços disponibilizados pela plataforma.

#### 4.3.3 Ganhos potencialmente gerados pelo fim da gratuidade compulsória

Como se pode observar, este modelo de regulação sugerido gera impactos substanciais nos modelos de negócio das plataformas. Busca-se, com isso, alcançar alguns resultados capazes de aumentar o nível de proteção dos dados pessoais dos usuários, incluindo efeitos que geram impactos superiores à proteção individual daquele que utiliza a plataforma com contraprestação em dinheiro. Nessa seção serão apresentados, sucintamente, alguns destes resultados esperados:

- a. **Fim do *take-it-or-leave-it-choice*.** Na realidade, significa o fim da cessão compulsória de um direito da personalidade para a celebração de um contrato, situação que, como já abordado, por si só constitui uma violação de Direito Fundamental. O usuário consumidor passa a ter uma opção efetivas de uso da plataforma, que não envolva seus dados pessoais como remuneração direta. As violações ao Direito do Consumidor e à Lei da Concorrência, com descritas na Seção 4.2.2, também são eliminadas com essa nova opção.
- b. **Parâmetros monetários claros para agregado de dados (dados pessoais como commodities).** Em geral, plataformas digitais não são transparentes na forma como calculam o valor dos dados agregados. Em 2019, os senadores americanos Mark Warner e Josh Hawley propuseram uma nova lei com o objetivo de obrigar as empresas de tecnologia, com mais de 100 milhões de usuários, a reportarem o valor dos dados pessoais coletados (SULLIVAN, 2019). Trata-se de uma pressão natural por um maior nível de transparência dos grandes *players* da internet, que costumam manter a opacidade de suas operações. A ideia da precificação, como apresentada na Seção 4.3.2.1, segue exatamente este princípio do valor agregado de dados, uma autodeclaração, pelo fornecedor, do volume financeiro total que representa o acervo geral de dados pessoais, mas aliado a este número ainda estabelece um modelo de precificação para de uso do serviço com remuneração direta, em dinheiro, e uma nova tributação que atinge os *players* de tecnologia, tendo como base de cálculo o valor-dados autodeclarado pela companhia.
- c. **Diminuição da efetividade das redes de capilaridade física e lógica.** A economia da vigilância está intimamente ligada à capacidade de perfilização e de entrega da mensagem publicitária ao perfil mais adequado, em uma busca constante pelo ideal mercado de um. Grande parte dos dados utilizados para essas finalidades não se originam do uso direto da plataforma, pelo indivíduo, mas são integrados a partir de outras aplicações, em uma grande e complexa teia de APIs

disponibilizadas por esses *players* para, justamente, promover essa captação de dados. Neste trabalho, chamamos essa teia de capilaridade lógica. Com o aumento do número dos dispositivos contendo sensores e atuadores, que tende a crescer de forma ainda mais expressiva com a IoT, expande-se também uma teia física, aqui denominada de capilaridade física, que também é utilizada para captação de dados pessoais e posterior integração com grandes plataformas, aumentando ainda mais a eficiência da perfilização. Ao cortar a associação destas informações capturadas na ponta às contas de usuário, nos moldes da decisão tomada pela autoridade antitruste alemã contra o Facebook, esses mecanismos de vigilância perdem força, aumentando o nível de proteção dos usuários finais.

**d. Mitigação dos efeitos de rede indiretos.** O grande volume de usuários pode, a depender do modelo de negócio, gerar efeitos de rede diretos e indiretos. Enquanto os efeitos diretos são percebidos em apenas alguns casos, os indiretos sempre existem, desde que se atinja a massa crítica necessária para poder desencadeá-los, no modelo de negócio das plataformas de dois ou múltiplos lados. O modelo de precificação apresentado na seção anterior tende a afetar os efeitos indiretos de rede, certamente com relação ao anunciante e, potencialmente, a outros *players* que ocupem outros lados da plataforma de múltiplos lados. Um usuário que não vê anúncios é irrelevante para o anunciante. Assim, quanto mais consumidores aderirem ao modelo de pagamento direto com dinheiro, menor será o nível de atratividade da plataforma para os anunciantes, abrindo espaço para outros competidores ou até outros veículos e mídias. A redução dos efeitos indiretos de rede também podem afetar outros lados, como os *publishers*, no caso das plataformas de disponibilização de anúncios (display), como o Google AdSense. Como há o impedimento de veiculação para o usuário que opta por não ter seus dados pessoais e sua atenção utilizadas para fins alheios à prestação de serviço, os espaços publicitários gerenciados pela plataforma em outros domínios também deverão ser bloqueados, o que geraria, naturalmente, uma menor propensão de uso das soluções de terceiros por parte dos publishers.

**e. Mitigação dos efeitos de escala de dados.** Apresentado na Seção 3.1.2.2, o efeito de escala de dados consiste em uma externalidade do lado da produção, citada por Stucke e Grunes (2017) como um dos componentes do que chamaram efeitos de rede orientada a dados (*data-driven network effects*), onde o grande volume de dados torna os serviços mais eficientes, com o tempo, à medida que são executados. Por esse motivo, também é conhecido por *learning by doing*. A eliminação da possibilidade de tratamento de dados pessoais baseado no legítimo interesse da plataforma ou de terceiros corta o fluxo de dados associado

ao perfil do usuário, que poderiam ser utilizados para perfilização e entrega de publicidade personalizada, reduzindo, esses efeitos de escala de dados. Visto de outro ângulo, as oportunidades de exposição de anúncios também desaparecem para esses usuários, eliminando a possibilidade de melhoria de desempenho a partir da recorrência de execução. Efeitos agregados, de diminuição da escala de dados de modo geral, abarcando os usuários que continuariam utilizando a versão gratuita, precisariam ser validados empiricamente.

- f. Melhor qualidade de informação para tomada de decisão sobre privacidade e proteção de dados.** Um dos aspectos mais relevantes ligados à capacidade de decisão dos indivíduos sobre a disposição de seus dados pessoais está ligado à dificuldade de entendimento de suas consequências, em grande medida derivada das características peculiares das transações envolvendo dados e privacidade, discutidas na Seção 3.1.1. O estabelecimento de um preço para a utilização da plataforma, sem que dados pessoais sejam utilizados como meio de remuneração direta, cria um ponto de comparação explícito, deixando claro que não há gratuidade, dando ao usuário uma baliza de valor, mesmo que indireta, do que está em sendo colocado como contrapartida. Também traz a sensação de que há um ônus contra o bônus de uso da plataforma, diminuindo, assim, os efeitos psicológicos do preço zero, tratados na Seção 3.1.2.3.
- g. Abrandamento da curva de faturamento frente à curva de usuários ativos.** Plataformas digitais podem apresentar curvas de faturamento que se comportam de maneira não linear, em uma função do número de usuários. Visto de um certo ponto de vista, significa que a receita gerada, tendo os dados pessoais como matéria prima, tende a aumentar de modo muito mais agressivo com o aumento do número de usuários, como demonstrado por Metcalfe (2013) no caso do Facebook, que apresenta crescimento quadrático. Esse fenômeno possivelmente está ligado a todas as externalidades positivas aproveitadas pelas plataformas, a partir da utilização dos mercados de dois ou múltiplos lados como modelo de negócio, que possibilitam a desassociação entre a entrega efetiva do serviço, para o cliente final, e os eventos geradores de receita, que acontecem por transação, em regra por leilão de espaços publicitários. Com a vinculação da receita ao usuário, eliminando os eventos geradores de receita não vinculados ao uso direto, a curva de crescimento de faturamento para esses serviços tende a ter comportamento mais linear, efeito da própria minimização do uso de dados pessoais como combustível para a geração de faturamento.
- h. Estímulos à concorrência.** As externalidades positivas aproveitadas pelas plataformas são, em grande medida, responsáveis pelo processo de concentração de mercado, que coloca as empresas em uma posição dominante ou até mo-



nopolista. Aplacar estas externalidades, mesmo que parcialmente, tende a criar um ambiente mais propício à concorrência. Além disso, o imposto baseado no valor-dados, conforme sugerido na Seção 4.3.2.1, também pode incentivar novos *players* a adotarem estratégias menos dependentes de dados pessoais, dando maior preferência para a remuneração direta, sem abrir mão dos clientes pouco sensíveis à proteção dos dados pessoais. Com um número maior de pagantes, a base de cálculo do imposto tenderá a ser menor, mesmo guardando-se as proporções, do que aquela experimentada pelos grandes *players*, cujos modelos de negócio são fixados, em grande medida, na remuneração direta por dados pessoais e não por dinheiro.

#### 4.3.4 Limitações do modelo

A principal limitação do modelo está na acentuação da desigualdade, entre pobres e ricos, no mundo digital. A posição de maior vulnerabilidade dos mais pobres já começa a ficar evidente. Como bem destaca Cathy O’Neil, matemática e autora do intrigante *Armas Matemáticas de Destruição* (*Weapon of Math Destruction*), os tratamentos computacionais tendem a penalizar os mais pobres, que serão mais submetidos a procedimentos automatizados do que os ricos, que terão acesso a relações mais pessoais (MENÁRGUEZ, 2018). O fator econômico age, portanto, como um redutor da quantidade de decisões automatizadas às quais as pessoas são submetidas. É exatamente este o caso dessa solução regulatória. A substituição da remuneração direta, baseada em dados, pela remuneração em dinheiro, cria uma oportunidade real de não perfilização e de preservação de uma esfera mais rígida de privacidade que poderá ser aproveitada apenas por aqueles que conseguirem pagar por isso. De toda maneira, mesmo com essa limitação importante, os efeitos coletivos do modelo, com a diminuição das externalidades, o aumento da transparência, a incidência de uma tributação sobre o valor-dados, o aumento da conscientização de que os dados pessoais têm valor e a possibilidade de entrada de novos competidores em mercados que, sem regulação específica, possuem grandes tendências monopolistas parecem justificar a sua adoção.

Há outras duas características que não são bem enquadradas como limitações, mas como dificuldades, e que, pela relevância, valem ser destacada. A primeira diz respeito a uma certa dificuldade de estabelecimento do valor-dados, para definição da base de cálculo para incidência do imposto. Em modelos mais simples, de tudo ou nada, como no caso do exemplo do Facebook, o valor-dados é fácil de ser calculado. Mas em algumas circunstâncias, as plataformas poderão adotar diversas ofertas diferentes, com níveis de uso de dados pessoais, baseados em legítimo interesse, também diferentes, já que não há vedação às ofertas que utilizam os dados pessoais como remuneração direta, seja total ou parcial. Nestes casos, o valor-dados precisaria

ser calculado levando em consideração os valores de cada oferta e a quantidade de usuários que optaram por cada uma delas. A segunda refere-se aos casos onde existe um grande concentrador de dados pessoais que opera um grande número de plataformas. É o caso do Google. É importante dar ao usuário a possibilidade de, em uma única oferta, optar pela não utilização dos dados pessoais como contrapartida à disponibilização de todo do *bundle* (pacote) de produtos. Isso pode gerar uma complicação operacional, devido à complexidade dos arranjos envolvendo diversas aplicações do mesmo fornecedor e suas integrações com outras aplicações, como no caso entre Google Maps e Uber, descrita na Seção 2.1.1. Vale ressaltar que o processo de geração massiva de dados, que resulta na economia da vigilância, é alimentado por esta mesma teia complexa que emaranha diversas aplicações. Neste sentido, desfazê-la para aumentar o nível de proteção do usuário dever ser, realmente, uma obrigação do dono da plataforma.

Importante considerar que esta é apenas uma primeira abordagem deste modelo de regulação baseado na vedação da gratuidade compulsória. Muitas outras limitações podem ser identificadas com a intensificação dos estudos sobre esse método de abordagem que objetiva aumentar a eficácia social dos Direitos Fundamentais relacionados aos dados pessoais.

## 5 CONCLUSÃO

A ideia de regulação de plataformas digitais traz consigo desafios imensos. Com grande poder computacional, formado por emaranhados complexos de sistemas, aplicações e infraestruturas, as plataformas movimentam modelos de negócio que aproveitam externalidades, raros nos setores tradicionais da economia, com potencial de torná-las cada vez mais dominantes em seus mercados.

Soluções tradicionais, na proteção à competição, são de difícil implementação ou não conseguiriam manter por muito tempo os resultados esperados. A alternativa clássica das cisões de empresas grandes demais, que passam a exercer um controle pernicioso do mercado, por exemplo, não parece ser viável para o caso das grandes plataformas. Isso ocorre, primeiro, porque é muito difícil, pela própria arquitetura dos serviços disponibilizados em rede, estabelecer onde deve ser realizado o corte preciso para viabilizar a separação. Segundo, porque a velocidade de expansão da capacidade de processamento torna essas medidas provisórias demais. Em outras palavras, a Lei de Moore joga contra essa categoria de solução.

Dia após dia, tentáculos conectados a estas plataformas se expandem em imensas teias que abrangem equipamentos e aplicações presentes em todos os cantos. Dentro de casa ou em qualquer outro lugar, cada indivíduo é monitorado, em maior ou menor grau, por diversos dispositivos que capturam dados e os integram às plataformas, mesmo sem que o usuário se dê conta disso. Todas essas informações são associadas ao seu perfil, que foi criado para dar-lhe acesso a serviços enganadoramente gratuitos.

No mundo da inovação disruptiva, as soluções para aumentar a eficácia dos Direitos Fundamentais ligados à proteção de dados deverão ser igualmente criativas. A integração entre Direito, design e engenharia se tornará inevitável. As garantias precisarão ser programadas, o que inevitavelmente deverá levar a uma regulação técnico-computacional mais rigorosa. A escalada de uso de *machine learning* também exigirá novas abordagens computacionais para que seja possível fazer o controle sobre as decisões tomadas automaticamente. Essas decisões, com impacto substancial a direitos e garantias, precisarão ser explicadas, em linguagem natural, de forma a viabilizar o entendimento e, inclusive, a contestação. Por isso, tendem a ganhar força conceitos como *accountable algorithms*, ou seja, mecanismos que possibilitem auditar as decisões computacionalmente tomadas, de forma a garantir que tais decisões encontram-se dentro dos limites legais e que não são violadoras de direitos.

O baixo nível de transparência, o comportamento *black box* das aplicações de *machine learning* são incompatíveis com os níveis de proteção aceitável aos Direitos Fundamentais e, por isso, abre-se a necessidade de empreender novos estudos em tecnologias que permitam dar maior clareza a esse tipo de decisão, como é o caso

da IA explicável, ou *explainable artificial intelligence*, que busca soluções para que as tomadas de decisão sejam acompanhadas por explicações racionais e inteligíveis por seres humanos (ADADI; BERRADA, 2018). Importante notar que esta capacidade está intrinsecamente ligada ao exercício dos direitos de explicação e revisão, que garantem aos titulares de dados pessoais o direito de receberem “informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial” (§ 1º, art. 20, da LGPD) e de solicitarem a revisão de decisões, tomadas unicamente por meio de tratamento automatizado de dados, que afetem os interesses do titular, incluindo aquelas “destinadas a definir o seu seu perfil pessoal, profissional, de consumo e de crédito ou os outros aspectos de sua personalidade” (art. 20, caput, LGPD). Por isso, o *enforcement* dos direitos de explicação e revisão passará por estabelecer exigências técnicas quanto à capacidade das próprias aplicações detalharem os motivos que levaram a uma determinada conclusão, sob pena de não cumprimento das obrigações legais estabelecidas pelas legislações de proteção de dados pessoais.

No campo puramente normativo, há necessidade de avanços consistentes, principalmente no Brasil. A alteração constitucional que explicita a garantia à proteção de dados como Direito Fundamental é um passo importante, mas seria ainda mais relevante se fosse acompanhada de uma declaração de direito de disposição sobre os próprios dados, preferencialmente mais abrangente do que a estabelecida no artigo 8.o, da Carta dos Direitos Fundamentais da União Europeia, eliminando a vinculação estreita com o consentimento, de modo a minimizar os paradoxos nascidos da incompreensão do caráter duplo dos dados pessoais, como partes da própria personalidade do indivíduo e, ao mesmo tempo, bens economicamente apreciáveis.

Alterações das legislações de proteção à competição, como a realizada na Alemanha, também podem ter efeitos favoráveis à proteção dos Direitos Fundamentais ligados à proteção de dados pessoais. Entender os efeitos de rede e de escala de dados, considerá-los nas avaliações de comportamento anti-competitivo e, principalmente, incorporar a privacidade e proteção de dados pessoais como elementos de qualidade, que precisam ser levados em consideração para a avaliação do bem estar do consumidor, permite atuações mais efetivas, onde a legislação antitruste age para aumentar o nível de proteção dos dados pessoais dos usuários finais. A decisão da autoridade alemã, no caso Facebook, é um exemplo lapidar de como esse sistema mais amplo de proteção pode funcionar.

As categorias do Direito do Consumidor também devem ser articuladas para garantir maior nível de proteção aos usuários, considerando a privacidade e a proteção de dados como partes integrantes de produtos e serviços, principalmente quando estas ofertas dependem de conexão, em tempo real, com serviços online, o que se tornará cada vez mais comum com o avanço da IoT.

Todas essas inovações normativas também favoreceriam a eficácia da alternativa de regulação apresentada neste trabalho. A vedação à gratuidade compulsória tem por objetivo dar ao indivíduo a possibilidade de exercício, da forma mais extensa possível nos dias de hoje, do direito de não dispor de seus dados pessoais. Vedar a utilização de dados pessoais baseada no legítimo interesse da plataforma ou de terceiros dá ao titular a opção de reduzir o nível de dispersão de seus dados, diminuindo sua vulnerabilidade a ações baseadas em marketing comportamental. Também pode gerar resultados relevantes na diminuição dos efeitos de rede, que são favorecidos pela não remuneração dos serviços, em dinheiro, pelos usuários finais, e na redução do efeito de escala de dados. Ao impedir que dados pessoais, capturados pelas teias de capilaridade lógica e física, sejam integrados ao perfil do usuário, combate-se, também, a ultra-perfilização, diminuindo a eficácia dos mecanismos que fazem a economia da vigilância funcionar.

Apesar de ser possível sustentar a vedação à gratuidade compulsória no contexto normativo atual, conforme explorado na Seção 4.2.2, é sempre bom não perder de vista que a sugestão de regulação aqui apresentada ainda é, apenas, um exercício teórico. Neste sentido, alinha-se a outros estudos que buscam, fora da aplicação tradicional das legislações específicas, alternativas para o aumento da eficácia social dos Direitos Fundamentais ligados à proteção dos dados pessoais.

A articulação dos diversos marcos normativos, a intensificação das regulações técnico-computacionais e as alterações regulatórias - da qual a proposta apresentada neste trabalho é um exemplo - que buscam alterar a dinâmica de mercados onde poucas empresas se favorecem pelo aproveitamento intensivo de várias externalidades, são iniciativas que precisam avançar não apenas em paralelo, mas que podem se complementar. Estudos que demonstrem os impactos e as consequências desta integração podem ser muito úteis para a construção de ambientes normativos e tecnológicos mais favoráveis aos Direitos Fundamentais.

No raiar da terceira década do século XXI, a visão de um controle absoluto das máquinas, do final do século passado, representado por *Matrix*, parece não passar de uma metáfora rasa. No delírio juvenil dos irmãos Wachowski, não são anacrônicos apenas a estética e os celulares com *flips* deslizantes. Baudrillard tinha razão em considerar *Show de Truman*, *Minority Report* e *Mulholland Drive* como expressões mais autênticas da interação simbiótica entre real e virtual, ao mesmo tempo que criticava *Matrix* por fazer uma separação explícita e contundente destes dois *ambientes* (FERREIRA, 2012).

Em um mundo cada vez mais dominado por plataformas, o hiperreal, de Baudrillard (1991), gerado por “modelos de um real sem origem nem realidade” está do outro lado, aquele onde os dados pessoais não são contornos de personalidade, mas substâncias imateriais manejadas como ativos de valor. Talvez, além da imbricação

do real e do virtual, exista, sim, um outro nível de existência, puramente digital, de representações de nós mesmos, que são articuladas de forma a influenciar nossa vida cotidiana mais prosaica. Na realidade, a luta contra a vigilância não acontece em Zion, mas nessa *Matrix Invertida* na qual vivemos.

## REFERÊNCIAS

ACQUISTI, Alessandro; TAYLOR, Curtis; WAGMAN, Liad. The Economics of Privacy. **Journal of Economic Literature**, v. 54, n. 2, p. 442–492, jun. 2016. ISSN 0022-0515. DOI: 10.1257/jel.54.2.442. Disponível em: <http://pubs.aeaweb.org/doi/10.1257/jel.54.2.442>.

ADADI, Amina; BERRADA, Mohammed. Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). **IEEE Access**, IEEE, v. 6, p. 52138–52160, 2018. ISSN 21693536. DOI: 10.1109/ACCESS.2018.2870052.

ALVES FILHO, Manuel. **Professor da Unicamp é um dos criadores da Iota**. Campinas: [s.n.], 2018. Disponível em: <https://www.unicamp.br/unicamp/noticias/2018/05/22/professor-da-unicamp-e-um-dos-criadores-da-iota>.

ALVES, Maria De Almeida. Directive on certain aspects concerning contracts for the supply of digital content and digital services & the EU data protection legal framework : are worlds colliding? v. 5, n. 2, p. 34–42, 2019.

AMAZON. **Amazon Prime chega ao Brasil em seu maior lançamento já feito em um país**. [S.l.]: Amazon, 2019. Disponível em: <https://www.amazon.com.br/b?ie=UTF8&node=19900334011>.

APPLE. **Introducing iPhone 11 Pro**. [S.l.: s.n.], 2019. Disponível em: <https://www.youtube.com/watch?v=cVEemOmHw9Y&feature=youtu.be&t=70>.

ARIELY, Dan. **Previsivelmente Irracional**. Rio de Janeiro: Elsevier Editora Ltda., 2008.

ARMBRUST, Michael *et al.* **Above the Clouds: A Berkeley View of Cloud Computing**. Berkeley, 2009. P. 25.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 4/2007 on the concept of personal data**. [S.l.], 2007.

ASIMOV, Isaac. **Segunda Fundação**. São Paulo: Aleph, 2009. ISBN 978-85-7657-068-4.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27701: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes, 2019.

BARBOSA MOREIRA, José Carlos. O Habeas data brasileiro e sua Lei regulamentadora. **Revista da EMERJ**, v. 1, n. 1, 1998.

BARROSO, Luiz André; DEAN, Jeffrey; HÖLZLE, Urs. Web search for a planet: The google cluster architecture. **IEEE Micro**, v. 23, n. 2, p. 22–28, 2003. ISSN 02721732. DOI: 10.1109/MM.2003.1196112.

BAUDRILLARD, Jean. **Simulacro e Simulação**. Lisboa: Antropos, 1991.

BECHTOLSHEIM, Andreas. **The Process of Innovation**. [S.l.: s.n.], 2012.

Disponível em: [https://www.youtube.com/watch?time\\_continue=2020&v=08frKEAtav4&feature=emb\\_logo](https://www.youtube.com/watch?time_continue=2020&v=08frKEAtav4&feature=emb_logo).

BECHTOLSHEIM, Andreas; BASKETT, Forest; PRATT, Vaughan. **The SUN Workstation Architecture**. [S.l.], 1982. Disponível em:

<http://i.stanford.edu/pub/cstr/reports/csl/tr/82/229/CSL-TR-82-229.pdf>.

BENJAMIN, Antônio Herman de V.; MARQUES, Cláudia Lima; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor**. 6a. Ed. São Paulo: Revista dos Tribunais, 2019. ISBN 978-8553213771.

BIONI, Bruno. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil**. São Paulo, 2015.

BOBEK, Michal. **Processo C-40/17. Conclusões do Advogado Geral**. [S.l.]: Tribunal de Justiça da União Europeia, 2019. Disponível em:

<http://curia.europa.eu/juris/document/document.jsf?docid=209357&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=PT&cid=4104426>.

BOERDING, Andreas *et al.* Data Ownership - A Property Rights Approach from a European Perspective. **Journal of Civil Law Studies**, v. 11, n. 2, p. 323–370, 2018.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. São Paulo: Malheiros, 2013.

BORGES, Jorge Luis. **Ficções**. São Paulo: Companhia das Letras, 1996.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. [S.l.: s.n.], 2002. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm).

BRASIL. **Lei nº 12.529, de 30 de novembro de 2011**. [S.l.: s.n.], 2011. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2011/Lei/L12529.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12529.htm).

BRASIL. **Lei nº 13.709, de 14 de Agosto de 2018**. [S.l.: s.n.], 2018. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm).

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. [S.l.: s.n.], 1990. Disponível em:

[http://www.planalto.gov.br/ccivil\\_03/leis/18078.htm](http://www.planalto.gov.br/ccivil_03/leis/18078.htm).



BRIN, Sergey; PAGE, Lawrence. Reprint of: The anatomy of a large-scale hypertextual web search engine. **Computer Networks**, Elsevier B.V., v. 56, n. 18, p. 3825–3833, 2012. ISSN 13891286. DOI: 10.1016/j.comnet.2012.10.007. Disponível em: <http://dx.doi.org/10.1016/j.comnet.2012.10.007>.

BUNDESKARTELLAMT. **Case Summary - Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing**. [S.l.: s.n.], 2019. Disponível em: <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html?nn=3591568>.

BUNDESKARTELLAMT. **Facebook, Exploitative business terms pursuant to Section 19(1) GWB for inadequate data processing**. [S.l.: s.n.], 2019.

CADE. **Resolução nº 20, de 9 de junho de 1999**. [S.l.], 1999.

CAMBRIDGE DICTIONARY. **Nomophobia**. [S.l.: s.n.], 2018. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/nomophobia>.

CANOTILHO, J. J. Gomes. **"Brançosos" e Interconstitucionalidade. Itinerários dos Discursos sobre a Historicidade Constitucional**. Lisboa: Almedina, 2008.

CAPELAS, Bruno. **Em busca de engenheiros, Nubank faz sua primeira aquisição**. [S.l.]: O Estado de São Paulo, jan. 2020. Disponível em: <https://link.estadao.com.br/noticias/inovacao,em-busca-de-engenheiros-nubank-faz-sua-primeira-aquisicao,70003146278>.

CASHMORE, Pete. **Network.com - Sun Provides Grid Computing for \$1/CPU-hour**. [S.l.: s.n.], 2006. Disponível em: <https://mashable.com/2006/03/22/networkcom-sun-launches-grid-computing-for-1cpu-hour/>.

CHAPPELOW, Jim. **Open Banking Definition**. [S.l.: s.n.], 2019. Disponível em: <https://www.investopedia.com/terms/o/open-banking.asp>.

CLEMONS, Eric K.; MADHANI, Nehal. Regulation of Digital Businesses with Natural Monopolies or Third-Party Payment Business Models: Antitrust Lessons from the Analysis of Google. **Journal of Management Information Systems**, v. 27, n. 3, p. 43–80, dez. 2010. ISSN 0742-1222. DOI: 10.2753/MIS0742-1222270303. Disponível em: <http://www.tandfonline.com/doi/full/10.2753/MIS0742-1222270303> <https://www.tandfonline.com/doi/full/10.2753/MIS0742-1222270303>.

CLOW, Lee. **The Real Story Behind Apple's Famous '1984' Super Bowl Ad**. [S.l.]: Bloomberg, 2014. Disponível em: <https://www.youtube.com/watch?v=PsjMmAqmb1Q>.

CNIL. **The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.** [S.l.]: CNIL, 2019. Disponível em:

<https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>.

COHEN, Julie E. **Between Truth and Power. The Legal Construction of Informational Capitalism.** New York: Oxford University Press, 2019. ISBN 9780190246716.

COHEN, Julie E. Networks, Standards, and Network-and-Standard-Based Governance. *In*: AFTER the Digital Tornado. [S.l.]: Cambridge University Press, 2019.

COHEN, Julie E. Surveillance Capitalism as Legal Entrepreneurship (Book Review). **Surveillance and Society**, v. 17, p. 240–245, 2019.

COHEN, Julie E. The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy. **Philosophy and Technology**, Philosophy & Technology, v. 31, n. 2, p. 213–233, 2018. ISSN 22105441. DOI: 10.1007/s13347-017-0258-2.

COHEN, Julie E. The regulatory state in the information age. **Theoretical Inquiries in Law**, v. 17, n. 2, p. 369–414, 2016. ISSN 15653404. DOI: 10.1515/ti1-2016-0015.

COHEN, Julie E. Turning privacy inside out. **Theoretical Inquiries in Law**, v. 20, n. 1, p. 1–31, 2019. ISSN 15653404. DOI: 10.1515/ti1-2019-0002.

COMMISSION 'COMPETITION LAW 4.0'. **A New Competition Framework for the Digital Economy.** [S.l.], 2019. Disponível em: [https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=3).

[https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.pdf?__blob=publicationFile&v=3).

CONIGLIO, Joseph. Why The ' New Brandeis Movement ' Gets Antitrust Wrong. **Law 360**, 2018. Disponível em: <https://ssrn.com/abstract=3166286>.

CROVITZ, Gordon. **Google Speaks Truth to Power.** [S.l.: s.n.], 2011. Disponível em: <https://www.wsj.com/articles/SB10001424052970204618704576645353164833940?ns=prod/accounts-wsj>.

DARRISAW, Michelle. **The 21 Best Songs to Wake Up to — Lovely Morning Songs.** [S.l.: s.n.], 2019. Disponível em: <https://www.oprahmag.com/entertainment/g26872626/best-songs-to-wake-up-to/>.

<https://www.oprahmag.com/entertainment/g26872626/best-songs-to-wake-up-to/>.

DELOITTE. **Global Mobile Consumer Survey Brasil 2018.** [S.l.], 2018.

Disponível em:

<https://www2.deloitte.com/content/dam/Deloitte/br/Documents/technology-media-telecommunications/Global-Mobile-Consumer-Survey-2018-Deloitte-Brasil.pdf>.

DELOITTE. **Global Mobile Consumer Survey Brasil 2019**. [S.l.], 2019. Disponível em: [http://images.e-mail.deloittecomunicacao.com.br/Web/DeloitteToucheTohmatsuAuditoresIndependente/%7B5ce7ce16-0c2a-4863-ba75-ad664b388600%7D\\_Global\\_Mobile\\_Consumer\\_Survey\\_Brasil\\_2019-Deloitte.pdf?utm\\_campaign=Global-Mobile-Consumer-Survey-2019-download&utm\\_med](http://images.e-mail.deloittecomunicacao.com.br/Web/DeloitteToucheTohmatsuAuditoresIndependente/%7B5ce7ce16-0c2a-4863-ba75-ad664b388600%7D_Global_Mobile_Consumer_Survey_Brasil_2019-Deloitte.pdf?utm_campaign=Global-Mobile-Consumer-Survey-2019-download&utm_med).

DELOITTE. **Pesquisa da Deloitte relata os hábitos dos brasileiros ao smartphone; mais de um terço deles acorda de madrugada e confere suas mensagens**. [S.l.: s.n.], 2016. Disponível em: <https://www2.deloitte.com/br/pt/footerlinks/pressreleasespage/Global-Mobile-Consumer-Survey-2016.html#>.

DENNEDY, Michelle Finneran; FOX, Jonathan; FINNERAN, Thomas R. **The Privacy Engineer's Manifesto. Getting from Policy to Code to QA to Value**. New York: Springer Science+Business Media, 2014.

DICIONÁRIO MICHAELIS. **Verbetes: consentimento**. [S.l.]: Editora Melhoramentos, 2020. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/consentimento/>.

DICK, Philip K. **Ubik**. São Paulo: Aleph, 2015. ISBN 978-85-7657-145-2.

DIXON, Helen. Statement of Helen Dixon, Commissioner, Data Protection Commission of Ireland. **Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework**, U.S. Senate Committee on Commerce, Science, e Transportation, p. 1–9, 2019.

DOMINGUES, Juliana Oliveira. **Big techs e o direito antitruste 4.0**. [S.l.: s.n.], 2019. Disponível em: <https://www1.folha.uol.com.br/opiniao/2019/06/big-techs-e-o-direito-antitruste-40.shtml>.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais. Fundamentos da Lei Geral de Proteção de Dados**. São Paulo: Revista dos Tribunais, 2019.

DORSEMAINE, Bruno *et al.* Internet of Things: A Definition and Taxonomy. *In*: September. 9TH International Conference on Next Generation Mobile Applications, Services and Technologies. Cambridge, UK: IEEE, 2015. P. 72–77. DOI: 10.1109/NGMAST.2015.71. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7373221&isnumber=7373199>.

DREXL, Josef. Designing Competitive Markets for Industrial Data - Between Propertisation and Access. **Max Planck Institute for Innovation & Competition Research Paper No. 16-13**, Max Planck Institute for Innovation e Competition, 2016. ISSN 1556-5068. DOI: 10.2139/ssrn.2862975. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2862975](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862975).

DUCH-BROWN, NNstor; MARTENS, Bertin; MUELLER-LANGER, Frank. The Economics of Ownership, Access and Trade in Digital Data. **JRC Digital Economy Working Paper 2017-01**, Joint Research Centre - European Commission, 2017. DOI: 10.2139/ssrn.2914144.

EADICICCO, Lisa. **Amazon Echo Buds preview: What it's like to use Amazon's new earbuds - Business Insider**. [S.l.: s.n.], 2019. Disponível em: <https://www.businessinsider.com/amazon-echo-buds-preview-hands-on-2019-9?r=US&IR=T>.

EDITORA MELHORAMENTOS. **Nomofobia**. [S.l.: s.n.], 2015. Disponível em: <https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/nomofobia/>.

EUROPA. **Diretiva (UE) 2019/790**. [S.l.: s.n.], 2019. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32019L0790>.

EUROPA. **Regulamento (UE) 2016/679**. [S.l.: s.n.], 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=celex%3A32016R0679>.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects**. [S.l.], 2019. P. 1–16. Disponível em: [https://edpb.europa.eu/sites/edpb/files/consultation/edpb\\_draft\\_guidelines-art\\_6-1-b-final\\_public\\_consultation\\_version\\_en.pdf](https://edpb.europa.eu/sites/edpb/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf).

EUROPEAN DATA PROTECTION BOARD. **Statement of the EDPB on the data protection impacts of economic concentration**. [S.l.]: European Data Protection Board, 2018. Disponível em: [https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-edpb-data-protection-impacts-economic-concentration\\_pt](https://edpb.europa.eu/our-work-tools/our-documents/autre/statement-edpb-data-protection-impacts-economic-concentration_pt).

EUROPEAN DATA PROTECTION SUPERVISOR. **Opinion 9/2016. EDPS Opinion on Personal Information Management Systems**. [S.l.], 2016.

EVANS, David S; SCHMALENSEE, Richard. The Antitrust Analysis of Multi-Sided Platform Businesses. **NBER Working Paper No. 18783**, National Bureau of Economics Research, 2013.

EZRACHI, Ariel; STUCKE, Maurice E. The fight over antitrust's soul. **Journal of European Competition Law & Practice**, v. 9, n. 1, p. 1–2, 2018. ISSN 2041-7764. DOI: 10.1093/jeclap/lpx070.

FACEBOOK. **Facebook Reports Fourth Quarter and Full Year 2019 Results**. [S.l.: s.n.], 2020. Disponível em:

<http://www.prnewswire.com/news-releases/facebook-reports-fourth-quarter-and-full-year-2015-results-300210893.html>.

FACEBOOK INC. **Termos de Serviço do Facebook**. [S.l.]: Facebook, 2019.

Disponível em: <https://www.facebook.com/terms>.

FAIRBAIRN, Douglas. **Oral History of Andreas “ Andy ” Bechtolsheim**. Mountain View, California: Computer History Museum, 2015.

FARRELL, Joseph. Can privacy be just another good? **Journal on Telecommunication & High Technology Law**, v. 10, p. 251–261, 2012.

Disponível em: [http://heinonlinebackup.com/hol-cgi-](http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jtelhtel10&section=20)

[bin/get\\_pdf.cgi?handle=hein.journals/jtelhtel10&section=20](http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jtelhtel10&section=20).

FERREIRA, Wilson. **Matrix revisitado: por que Jean Baudrillard não gostou do filme?** [S.l.: s.n.], 2012. Disponível em:

<https://revistaforum.com.br/blogs/cinegnose/matrix-revisitado-por-que-jean-baudrillard-nao-gostou-do-filme/>.

GARFINKEL, Simson L. **Architects of the information society: 35 years of the Laboratory for Computer Science at MIT**. Cambridge, Mass.: Massachusetts Institute of Technology, 1999.

GERMAN. Act Against Restraints of Competition. **Federal Law Gazette**, Bundeskartellamt, 2013.

GIBSON, James J. The theory of affordances. *In*: THE Ecological Approach to Visual Perception. Classic Ed. New York: Psychology Press, 2015.

GILDER, George. **The Gilder Paradigm**. [S.l.: s.n.], 1996. Disponível em:

<https://www.wired.com/1996/12/gilder-3/>.

GINGRAS, Richard. **How Google invests in news**. [S.l.]: Google, 2019.

Disponível em: <https://blog.google/perspectives/richard-gingras/how-google-invests-news/>.

GLOBALSTATS. **Browser Market Share**. [S.l.: s.n.], 2020. Disponível em:

<https://gs.statcounter.com/browser-market-share/>.

GLOBALSTATS. **Mobile Operating System Market Share Worldwide**. [S.l.: s.n.], 2020. Disponível em:

<https://gs.statcounter.com/os-market-share/mobile/worldwide>.

GOLDFARB, Avi. What is Different About Online Advertising? **Review of Industrial Organization**, v. 44, n. 2, p. 115–129, 2014. ISSN 15737160. DOI:

10.1007/s11151-013-9399-3.

GOLDFARB, Avi; TUCKER, Catherine. Digital economics. **Journal of Economic Literature**, v. 57, n. 1, p. 3–43, 2019. ISSN 00220515. DOI: 10.1257/jel.20171452.

GOOGLE. **Formalizing the Robots Exclusion Protocol Specification**. [S.l.]: Google, 2019. Disponível em:  
<https://webmasters.googleblog.com/2019/07/rep-id.html>.

GOOGLE LLC. **Termos de Serviço do Google**. [S.l.]: Google, 2017. Disponível em:  
<https://policies.google.com/terms?hl=pt-BR>.

GRAU, Eros Roberto. **A Ordem Econômica na Constituição de 1988**. 18ª Ed. São Paulo: Malheiros, 2018.

GRIMMELMANN, James. The Platform is the Message. **Georgetown Law Technology Review**, v. 2, n. 2, 2018.

GRINOVER, Ada Pellegrini *et al.* **Código Brasileiro de Defesa do Consumidor. Comentado pelos Autores do Anteprojeto**. 11ª. Rio de Janeiro: Forense, 2017. ISBN 978-85-309-6064-3.

HALLIDAY, David; RESNICK, Robert; WALKER, Jearl. **Fundamentos de Física 4**. 4a. Ed. Rio de Janeiro: LTC - Livros Técnicos e Científicos Editora S.A., 1995.

HARBOR, Cara. **Part 1: IOTA Data Marketplace — Update**. [S.l.: s.n.], 2019. Disponível em:  
<https://blog.iota.org/part-1-iota-data-marketplace-update-5f6a8ce96d05>.

HASHAI, Niron. Platform End Users as Free 'Data Labor' - Re-Distributing the Value Created in Double Sided Markets. **SSRN Electronic Journal**, p. 1–24, 2018. ISSN 1556-5068. DOI: 10.2139/ssrn.3121160. Disponível em:  
<https://www.ssrn.com/abstract=3121160>.

HESTNESS, Joel *et al.* Deep Learning Scaling is Predictable, Empirically. **arXiv.org**, p. 1–19, 2017. Disponível em: <http://arxiv.org/abs/1712.00409>.

HEYER, Ken; SHAPIRO, Carl; WILDER, Jeffrey. The year in review: Economics at the antitrust division, 2008-2009. **Review of Industrial Organization**, v. 35, n. 4, p. 349–367, 2009. ISSN 0889938X. DOI: 10.1007/s11151-009-9232-1.

HILDEBRANDT, Mireille. Law As an Affordance : The Devil Is in the Vanishing Point ( s ). **Critical Analysis of Law**, v. 4, n. 1, p. 116–128, 2017.

HILDEBRANDT, Mireille. **Smart technologies and the end (s) of law: novel entanglements of law and technology**. Cheltenham: Edward Elgar Publishing, 2015.

IBARRA, Imanol Arrieta *et al.* Should We Treat Data as Labor? Moving Beyond Free. **AEA Papers and Proceedings**, American Economic Association, v. 108, p. 38–42, 2018.

IBGE. **PNAD Contínua 2017 - Acesso à Internet e Posse de Telefone Móvel Celular para Uso Pessoal**. Brasília, 2018. Disponível em:

<https://agenciadenoticias.ibge.gov.br/agencia-detalle-de-midia.html?view=mediaibge&catid=2103&id=2599>.

ICO. **Guidance on the rules on use of cookies and similar technologies**.

[S.l.: s.n.], jul. 2019. Disponível em: <https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/#comply7>.

ICO. **Update report into adtech and real time bidding**. [S.l.], 2019.

IDC. **IDC Forecasts Worldwide Technology Spending on the Internet of Things to Reach \$1.2 Trillion in 2022**. [S.l.: s.n.], 2018. Disponível em:

<https://www.idc.com/getdoc.jsp?containerId=prUS43994118>.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. CNAE 213-5 - Empresário (individual). **Site da Comissão Nacional de Classificação**, 2018.

Disponível em: <https://concla.ibge.gov.br/estrutura/natjur-estrutura/natureza-juridica-2018/23246-213-5-empresario-individual>.

INTEL CORPORATION. **The Story of the Intel® 4004**. [S.l.: s.n.]. Disponível em:

<https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html>.

IOTA FOUNDATION. **The IOTA Vision**. [S.l.: s.n.]. Disponível em:

<https://www.iota.org/the-foundation/our-vision>.

IRVINE, Mark. **Google Ads Benchmarks for YOUR Industry [Updated!]** [S.l.]: WordStream, 2019. Disponível em:

<https://www.wordstream.com/blog/ws/2016/02/29/google-adwords-industry-benchmarks>.

ISAACSON, Walter. **Os Inovadores**. São Paulo: Companhia das Letras, 2014. ISBN 978-85-438-0186-5.

JANECEK, V; MALGIERI, G. Commerce in data and the dynamically limited alienability rule. **German Law Journal**, Cambridge University Press, v. 21, p. 1–20, 2019. ISSN 2071-8322. DOI: 10.31228/osf.io/7ztys.

KEMP, Simon. **Digital 2019. Essential insights into how people around the world use the internet, mobile devices, social media, and e-commerce.** [S.l.: s.n.], 2019. P. 77. Disponível em: <https://datareportal.com/reports/digital-2019-brazil>.

KHAN, Lina M. Amazon's antitrust paradox. **Yale Law Journal**, v. 126, n. 3, p. 710–805, 2017. ISSN 00440094.

KIRA, Beatriz. A Defesa da Concorrência na Era Digital: Desafios Práticos e Teóricos em Face das Plataformas de Internet. **Revista de Direito e Novas Tecnologias**, Revista dos Tribunais, v. 2, 2019.

KNIGGE, Michael. **Von Bechtolsheim: I invested in Google to solve my own problem.** [S.l.: s.n.], 2009. Disponível em: <https://www.dw.com/en/von-bechtolsheim-i-invested-in-google-to-solve-my-own-problem/a-4557608>.

KONRAD, Alex. **The Best Startup Accelerators Of 2017.** [S.l.: s.n.], jun. 2017. Disponível em: <https://www.forbes.com/sites/alexkonrad/2017/06/07/best-accelerators-of-2017/#57e6927610cb>.

KOOPS, Bert Jaap. The trouble with European data protection law. **International Data Privacy Law**, Oxford University Press, v. 4, n. 4, p. 250–261, 2014. ISSN 20444001. DOI: 10.1093/idpl/ipu023.

KOSTER, Martijn. **Robots.txt is 25 years old.** [S.l.: s.n.], 2019. Disponível em: <https://www.greenhills.co.uk/posts/robotstxt-25/>.

KRISTOL, David M. HTTP Cookies: Standards, Privacy, and Politics. **ACM Transactions on Internet Technology**, v. 1, n. 2, p. 151–198, 2001. ISSN 15576051. DOI: 10.1145/502152.502153.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica.** 8a. Ed. São Paulo: Editora Atlas, 2017.

LANIER, Jaron. **Who Owns the Future.** New York: Simon & Schuster, 2013.

LEVY, Steven. **Google a biografia.** São Paulo: Universo dos Livros Editora, 2012. ISBN 978-85-7930-286-2.

LEWIS, C. S. **Sobre Histórias.** Rio de Janeiro: Thomas Nelson Brasil, 2018.

LI, Shancang; XU, Li Da; ZHAO, Shanshan. The internet of things: a survey. **Information Systems Frontiers**, v. 17, n. 2, p. 243–259, 2015. ISSN 13873326. DOI: 10.1007/s10796-014-9492-7.



LYFT. **IPO Filing**. [S.l.: s.n.], 2019. Disponível em: <https://www.sec.gov/Archives/edgar/data/1759509/000119312519059849/d633517ds1.htm>.

LYNSKEY, Orla. **Data Protection Through the Looking Glass**. [S.l.]: nic.br, 2019. Disponível em: <https://www.youtube.com/watch?v=CeT02X47Wqg>.

LYNSKEY, Orla. Grappling with "data power": Normative nudges from data protection and privacy. **Theoretical Inquiries in Law**, v. 20, n. 1, p. 189–220, 2019. ISSN 15653404. DOI: 10.1515/ti1-2019-0007.

MALGIERI, Gianclaudio; CUSTERS, Bart. Pricing privacy – the right to know the value of your personal data. **Computer Law and Security Review**, Elsevier Ltd, v. 34, n. 2, p. 289–303, 2018. ISSN 02673649. DOI: 10.1016/j.clsr.2017.08.006. Disponível em: <https://doi.org/10.1016/j.clsr.2017.08.006>.

MARCHETTI, Brunno. **Como Decolar.com e outras empresas mudam preços de acordo com seus dados**. [S.l.]: Vice, 2018. Disponível em: [https://www.vice.com/pt\\_br/article/kzpyvz/como-decolarcom-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados](https://www.vice.com/pt_br/article/kzpyvz/como-decolarcom-e-outras-empresas-mudam-precos-de-acordo-com-seus-dados).

MCCARTHY, John. **The Home Information Terminal - a 1970 View**. [S.l.], 2000. P. 1–12.

MCLUHAN, Marshall; FIORE, Quentin. **O meio é a mensagem: um inventário de efeitos**. Rio de Janeiro: Imã Editorial, 2011.

MENÁRGUEZ, Ana Torres. **“Os privilegiados são analisados por pessoas; as massas, por máquinas”**. [S.l.: s.n.], 2018. Disponível em: [https://brasil.elpais.com/brasil/2018/11/12/tecnologia/1542018368\\_035000.html](https://brasil.elpais.com/brasil/2018/11/12/tecnologia/1542018368_035000.html).

MESSINA, Chris. **Groups for Twitter; or A Proposal for Twitter Tag Channels**. [S.l.: s.n.], 2007. Disponível em: <https://factoryjoe.com/2007/08/25/groups-for-twitter-or-a-proposal-for-twitter-tag-channels/>.

METCALFE, Bob. Metcalfe’s law after 40 years of ethernet. **Computer**, v. 46, n. 12, p. 26–31, 2013. ISSN 00189162. DOI: 10.1109/MC.2013.374.

MEZZAROBA, Orides; MONTEIRO, Claudia Servilha. **Manual de metodologia da pesquisa no Direito**. 15a. Ed. São Paulo: Editora Saraiva, 2017.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, Revista dos Tribunais, p. 1–35, 2019.

MIRAGEM, Bruno. Direito do Consumidor e Ordenação do Mercado. O Princípio da Defesa do Consumidor e sua Aplicação na Regulação da Propriedade Intelectual,

Livre Concorrência e Proteção do Meio Ambiente. **Revista do Direito do Consumidor**, Revista dos Tribunais, 2012.

MIYAZAWA, Flávio Keidi. **Introdução à Teoria dos Jogos Algorítmica**. Campinas, 2010. Disponível em:

<https://www.ic.unicamp.br/~fkm/lectures/algorithmicgametheory.pdf>  
<http://www.ic.unicamp.br/~fkm/lectures/algorithmicgametheory.pdf>.

MYERS, Andrew. **Andy Bechtolsheim: Hero talks innovation, success and engineering**. [S.l.: s.n.], 2012. Disponível em:

<https://engineering.stanford.edu/news/andy-bechtolsheim-engineering-hero-talks-innovation-success-and-engineering>.

NOBELPRIZE.ORG. **The Nobel Prize in Physics 1922**. [S.l.]: NobelPrize.org, 2020. Disponível em: <https://www.nobelprize.org/prizes/physics/1922/summary/>.

NORMAN, Donald A. **The design of everyday things**. New York: Basic Books, 2013. P. 1. ISBN 9780465050659.

NOVET, Jordan. **Uber paid Google \$58 million over three years for map services**.

[S.l.: s.n.], 2019. Disponível em: <https://www.cnn.com/2019/04/11/uber-paid-google-58-million-over-three-years-for-map-services.html>.

NUNES, Rizzatto. **Curso de Direito do Consumidor**. 13a. Ed. São Paulo: Editora Saraiva, 2019. ISBN 9788553607525.

O'REILLY, Tim. **Amazon Web Services API**. [S.l.: s.n.], 2002. Disponível em:

<https://web.archive.org/web/20110709221736/http://www.oreillynet.com/pub/wlg/1707?wlg=yes>.

O'REILLY, Tim. **Web 2.0 Compact Definition: Trying Again**. [S.l.: s.n.], 2006.

Disponível em: <https://web.archive.org/web/20090123232944/http://radar.oreilly.com/archives/2006/12/web-20-compact.html>.

O'REILLY, Tim. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. **Communications E Strategies**, n. 65, 2007.

OLSON, Parmy. **European Regulators Target Big Tech Companies**. [S.l.: s.n.],

2020. Disponível em: <https://www.wsj.com/articles/european-regulators-target-big-tech-companies-11579542357>.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2019.

ORWELL, George. **Como morrem os pobres e outros ensaios**. São Paulo: Companhia das Letras, 2009.

OXFORD ENGLISH DICTIONARY. **New words list October 2019**. [S.l.: s.n.], 2019. Disponível em: <https://public.oed.com/updates/new-words-list-october-2019/>.

PAGE, Lawrence *et al.* **The PageRank Citation Ranking: Bringing Order to the Web**. [S.l.], 1999. Disponível em: <http://ilpubs.stanford.edu:8090/422/>.

PARLAMENTO EUROPEU. Disposições de Direito Civil sobre Robótica. **Jornal Oficial da União Europeia**, 2017. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//PT#BKMD-12%20http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN>.

PASQUALE, Frank. Privacy, Antitrust, and Power. **George Mason Law Review**, v. 20, 2013.

PASQUIER, Thomas; EYERS, David; BACON, Jean. Viewpoint personal data and the internet of things. **Communications of the ACM**, v. 62, n. 6, p. 32–34, 2019. ISSN 15577317. DOI: 10.1145/3322933.

PASQUIER, Thomas; SINGH, Jatinder *et al.* Data provenance to audit compliance with privacy policy in the Internet of Things. **Personal and Ubiquitous Computing, Personal e Ubiquitous Computing**, v. 22, n. 2, p. 333–344, 2018. ISSN 16174909. DOI: 10.1007/s00779-017-1067-4.

PASSOS JR., Osvaldo. **Demônio de Maxwell e a Física da Computação**. [S.l.]: Universidade de São Paulo, 2017. Disponível em: <http://opessoa.fflch.usp.br/FiFi-17>.

PENTLAND, Alex Sandy. The Data-Driven Society. **Scientific American**, v. 309, n. 4, p. 78–83, 2013.

PEREIRA, Alexandre L Dias. Novos direitos do consumidor no mercado único digital. **Estudos de Direito do consumidor**, Coimbra, v. 10, 2016.

PORTER, Michael E.; HEPPELMANN, James E. How smart, connected products are transforming companies. **Harvard Business Review**, v. 93, n. 10, p. 06–114, out. 2015. ISSN 00178012. Disponível em: <http://web.a.ebscohost.com/ehost/detail/detail?vid=9&sid=d9b0438d-44aa-4162-b3b8-b5283b973c4e%40sessionmgr4010&bdata=Jmxhbm9cHQtYnImc210ZT11aG9zdC1saXZl#>.

PORTER, Michael E.; HEPPELMANN, James E. How smart, connected products are transforming competition. **Harvard Business Review**, v. 92, n. 11, p. 64–88, nov. 2014. ISSN 00178012. Disponível em: <http://web.a.ebscohost.com/ehost/detail/detail?vid=11&sid=d9b0438d-44aa->

4162-b3b8-

b5283b973c4e%40sessionmgr4010&bdata=Jmxhbmc9cHQYnImc2l0ZT1laG9zdC1saXZl#.

POSNER, Eric; WEYL, E. Glen. **Mercados Radicais. Reinventando o Capitalismo e a Democracia para uma Sociedade Mais Justa**. São Paulo: Portfolio-Penguin, 2019. ISBN 978-85-8285-093-1.

POSNER, Richard A. **A Economia da Justiça**. 1ª Ed. São Paulo: WMF Martins Fontes, 2010. ISBN 9788578271237.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, Taylor & Francis, v. 10, n. 1, p. 40–81, 2018. ISSN 1757997X. DOI: 10.1080/17579961.2018.1452176.

RIES, Eric. **A Total Disruption Interviews**. [S.l.: s.n.], 2015. Disponível em: [http://getanswers.atotaldisruption.com/media/Eric+Ries+-+Lean+Startup/0\\_h2792k72](http://getanswers.atotaldisruption.com/media/Eric+Ries+-+Lean+Startup/0_h2792k72).

ROCCA, Pablo; BRIZ, María de los Ángeles González. **Fray Bentos**. [S.l.]: Companhia das Letras, 2017.

ROCCA, Pablo; BRIZ, María de los Ángeles González. **Ipuche, Pedro Leandro**. [S.l.]: Companhia das Letras, 2017.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**. Rio de Janeiro: Renovar, 2008. ISBN 978-85-7147-688-2.

ROUGHGARDEN, Tim. **CS269I : Incentives in Computer Science. Lecture # 15: The VCG Mechanism**. New York: [s.n.], 2016. P. 1–10. Disponível em: <http://timroughgarden.org/f16/1/115.pdf>.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. **Direito, Estado e Sociedade**, n. 36, p. 178–199, 2010.

RUSHE, Dominic. **Google News Spain to close in response to story links 'tax'**. [S.l.]: The Guardian, 14.

SADASHIV, Naidila; KUMAR, S. M. Dilip. Cluster, grid and cloud computing: A detailed comparison. **ICCSE 2011 - 6th International Conference on Computer Science and Education, Final Program and Proceedings**, p. 477–482, 2011. DOI: 10.1109/ICCSE.2011.6028683.

SADOWSKI, Jathan. **Why Silicon Valley is embracing universal basic income**. [S.l.: s.n.], jun. 2016. Disponível em:

<https://www.theguardian.com/technology/2016/jun/22/silicon-valley-universal-basic-income-y-combinator>.

SARACCO, Roberto. **1.2 trillion transistor on a chip to fuel AI**. Piscataway, NJ: [s.n.], 2019. Disponível em:

<https://cmt.eiee.org/futuredirections/2019/08/31/1-2-trillion-transistor-on-a-chip-to-fuel-ai/>.

SCHINDLER, Philipp. **The Google News Initiative: Building a stronger future for news**. [S.l.]: Google, 2018. Disponível em: <https://www.blog.google/outreach-initiatives/google-news-initiative/announcing-google-news-initiative/>.

SCHUH, Justin. **Building a more private web: A path towards making third party cookies obsolete**. [S.l.]: Google, 2020. Disponível em: <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: Privacy and a new concept of personally identifiable information. **New York University Law Review**, v. 86, n. 6, p. 1814–1894, 2011. ISSN 00287881.

SEABRA, Antonio Carlos. **Atuadores. Aula 26**. [S.l.: s.n.], 2016. Disponível em: <https://www.youtube.com/watch?v=LCbGD2nA1rg>.

SEARLS, Doc. **The intention economy : when customers take charge**. Cambridge, Mass.: Harvard Business Review Press, 2012.

SHAMPANIER, Kristina; MAZAR, Nina; ARIELY, Dan. Zero as a special price: The true value of free products. **Marketing Science**, v. 26, n. 6, p. 742–757, 2007. ISSN 07322399. DOI: 10.1287/mksc.1060.0254.

SHAPIRO, Carl; VARIAN, Hal R. **Information Rules**. Boston: Harvard Business School Press, 1999. v. 32. ISBN 087584863X.

SHNEIDERMAN, Ben. **Algorithmic Accountability: Design for Safety**. [S.l.]: Harvard University, 2018. Disponível em: <https://www.youtube.com/watch?v=H2iiHiK-hJ0>.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 1994.

SLEFO, George P. **Google called out by ANA and 4A's after saying it will phase out cookies from Chrome**. [S.l.]: AdAge, 2020. Disponível em:

<https://adage.com/article/digital/google-called-out-ana-and-4as-after-saying-it-will-phase-out-cookies-chrome/2227931>.



TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. **Processo T-201/04**. [S.l.: s.n.], 2007. Disponível em:

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=62940&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=5228129>.

TRUETT, Lila J.; TRUETT, Dale B. **Managerial Economics**. Hoboken, NJ: John Wiley e Sons, Inc., 2004.

TUCKER, Catherine. Network Effects and Market Power: What Have We Learned in the Last Decade? **Antitrust**, 2018.

UBER TECHNOLOGIES. **IPO Filing**. [S.l.: s.n.], 2019. Disponível em:

[https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm#toc647752\\_9](https://www.sec.gov/Archives/edgar/data/1543151/000119312519103850/d647752ds1.htm#toc647752_9).

UNITED STATES OF AMERICA. Open data policy: Managing information as an asset. **Office of Management Budget. Executive Office of The Presidente of the United States**, Washington, DC, 2013.

VARIAN, Hal R. Artificial Intelligence, Economics, and Industrial Organization. **NBER Working Paper No. 24839**, National Bureau of Economics Research, Cambridge, Mass., 2018. ISSN 0013-1857.

VARIAN, Hal R. **Biografia de Hal R. Varian**. [S.l.: s.n.]. Disponível em:

<http://people.ischool.berkeley.edu/~hal/people/hal/biography.html>.

VARIAN, Hal R. Designing the perfect auction. **Communications of the ACM**, v. 51, n. 8, p. 9–11, 2008. ISSN 00010782. DOI: 10.1145/1378704.1378708.

VARIAN, Hal R. **Introdução ao Leilão do Google**. [S.l.]: Google Brasil, 2009.

Disponível em: [https://www.youtube.com/watch?v=Fg01uSe72lc&feature=emb\\_logo](https://www.youtube.com/watch?v=Fg01uSe72lc&feature=emb_logo).

VARIAN, Hal R. **Macroeconomia: uma abordagem moderna**. São Paulo: Elsevier Editora Ltda., 2015.

VARIAN, Hal R. Recent Trends in Concentration, Competition, and Entry. **Antitrust Law Journal**, v. 82, n. 3, p. 807–834, 2019. Disponível em:

<https://widgets.ebscohost.com/prod/customerspecific/s7060880/novo-acesso/index.php?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139262763&lang=pt-br&site=ehost-live&scope=site&authtype=ip>.

VARIAN, Hal R. The economics of Internet search. **Rivista di Politica Economica**, 2006.

VARIAN, Hal R.; FARRELL, Joseph; SHAPIRO, Carl. **The Economics of Information Technology. A introduction.** Cambridge, UK: Cambridge University Press, 2004.

VERTO ANALYTICS. **Most popular mapping apps in the United States as of April 2018, by reach.** [S.l.: s.n.], 2019. Disponível em:

<https://www.statista.com/statistics/865419/most-popular-us-mapping-apps-ranked-by-reach/>.

VINOCUR, Nicholas. **'We have a huge problem': European tech regulator despairs over lack of enforcement.** [S.l.]: Politico, 2019. Disponível em:

<https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605>.

WISE, David A.; MALSEED, Mark. **The Google Story.** New York: Bantam Books, 2018. ISBN 9780440335702.

WALLIN, Leif-Olof. **IoT Opportunities and Challenges in 2019 and Beyond.**

[S.l.: s.n.], 2019. Disponível em: [http:](http://public2.brighttalk.com/resource/core/239869/sep12lwallin-_529032.pdf)

[//public2.brighttalk.com/resource/core/239869/sep12lwallin-\\_529032.pdf](http://public2.brighttalk.com/resource/core/239869/sep12lwallin-_529032.pdf).

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193–220, dez. 1890.

WECKLER, Adrian. **Data breaches in Ireland 'amongst highest in the EU'.**

[S.l.: s.n.], jan. 2020. Disponível em:

<https://www.independent.ie/business/technology/gdpr/data-breaches-in-ireland-amongst-highest-in-the-eu-38875532.html>.

WEIZENBAUM, Joseph. ELIZA - a computer program for the study of natural language communication between man and machine. **Communications of the ACM**, v. 9, n. 1, p. 36–45, jan. 1966.

WENGER, Albert. **A BIG idea, a bot idea. How smart policy will advance tec.** New York: [s.n.], 2015. Disponível em: [https://www.youtube.com/watch?v=t8qo7pzH\\_NM](https://www.youtube.com/watch?v=t8qo7pzH_NM).

WENGER, Albert. Universal Basic Income: An Introduction. *In: 72ND Annual NYU Labor Conference.* [S.l.: s.n.], 2019. Disponível em:

<https://continuations.com/post/185978039865/universal-basic-income-an-introduction>.

WHATSAPP INC. **Política de privacidade do WhatsApp.** [S.l.]: WhatsApp Inc., 2019. Disponível em:

[https://www.whatsapp.com/legal?eea=0&lang=pt\\_br#terms-of-service](https://www.whatsapp.com/legal?eea=0&lang=pt_br#terms-of-service).

WORLD ECONOMIC FORUM. **Competition Policy in a Globalized , Digitalized Economy.** [S.l.], 2019.



WP29 - ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 8/2014 on the on Recent Developments on the Internet of Things**. Brussels, 2014.

WU, Tim. **In the Grip of the New Monopolists**. [S.l.: s.n.], 2010. Disponível em: <https://www.wsj.com/articles/SB10001424052748704635704575604993311538482>.

Y COMBINATOR RESEARCH. **Basic Income Project Proposal**. [S.l.], 2017. Disponível em: <https://static1.squarespace.com/static/599c23b2e6f2e1aeb8d35ec6/t/59c3188c4c326da3497c355f/1505958039366/YCR-Basic-Income-Proposal.pdf>.

YC RESEARCH. **Our Plan**. [S.l.]: Y Combinator. Disponível em: <https://basicincome.ycr.org/our-plan>.

ZHANG, Xing Zhou; LIU, Jing Jie; XU, Zhi Wei. Tencent and Facebook Data Validate Metcalfe's Law. **Journal of Computer Science and Technology**, v. 30, n. 2, p. 246–251, 2015. ISSN 10009000. DOI: 10.1007/s11390-015-1518-1.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. London: Profile Books Ltd, 2019.

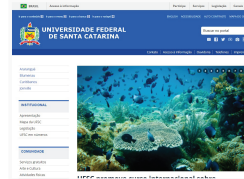
## ANEXO A – RELATÓRIO DE VARREDURA DE COOKIES



### Cookie scan report

#### Summary

Scan date: 15/01/2020  
 Domain name: ufsc.br  
 Server location: Brazil  
 Cookies, in total: 14



#### Scan result

14 cookies were identified.  
 1 cookies are unclassified and need manual classification and a purpose description.

**The result is based on a scan of up to 5 website pages and therefore not complete. To perform a complete scan, create a Cookiebot subscription for your domain.**

#### Category: Necessary (2)

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

COOKIE NAME	PROVIDER	TYPE	EXPIRY
PHPSESSID	noticias.ufsc.br	HTTP	Session
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a> <b>Cookie purpose description:</b> Preserves user session state across page requests. <b>Initiator:</b> Webserver <b>Source:</b> noticias.ufsc.br <b>Data is sent to:</b> Brazil (not adequate)			
PHPSESSID	ufsc.br	HTTP	Session
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a> <b>Cookie purpose description:</b> Preserves user session state across page requests. <b>Initiator:</b> Webserver <b>Source:</b> ufsc.br <b>Data is sent to:</b> Brazil (not adequate)			

#### Category: Marketing (11)

Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby more valuable for publishers and third party advertisers.

COOKIE NAME	PROVIDER	TYPE	EXPIRY
GPS	youtube.com	HTTP	1 day
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a> <b>Cookie purpose description:</b> Registers a unique ID on mobile devices to enable tracking based on geographical GPS location. <b>Initiator:</b> IFRAME, page source line number 558 <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;wmode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;wmode=transparent</a> <b>Data is sent to:</b> United States (adequate) Adequate country under GDPR (EU) <b>Blocked until accepted by user:</b> No			
IDE	doubleclick.net	HTTP	1 year
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a> <b>Cookie purpose description:</b> Used by Google DoubleClick to register and report the website user's actions after viewing or clicking one of the advertiser's ads with the purpose of measuring the efficacy of an ad and to present targeted ads to the user.			

<p><b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>test_cookie</b>	doubleclick.net	HTTP	1 day
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Used to check if the user's browser supports cookies.  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>VISITOR_INFO_LIVE</b>	youtube.com	HTTP	179 days
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Tries to estimate the users' bandwidth on pages with integrated YouTube videos.  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>YSC</b>	youtube.com	HTTP	Session
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Registers a unique ID to keep statistics of what videos from YouTube the user has seen.  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>yt-remote-cast-installed</b>	youtube.com	HTML	Session
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>yt-remote-connected-devices</b>	youtube.com	HTML	Persistent
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>yt-remote-device-id</b>	youtube.com	HTML	Persistent
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)  Adequate country under GDPR (EU)  <b>Blocked until accepted by user:</b> No</p>			
<b>yt-remote-fast-check-period</b>	youtube.com	HTML	Session
<p><b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>  <b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video  <b>Initiator:</b> Iframe, page source line number 558  <b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=darkcolor=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>  <b>Data is sent to:</b> United States (adequate)</p>			

Adequate country under GDPR (EU)			
<b>Blocked until accepted by user:</b> No			
<b>yt-remote-session-app</b>	youtube.com	HTML	Session
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>			
<b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video			
<b>Initiator:</b> IFrame, page source line number 558			
<b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>			
<b>Data is sent to:</b> United States (adequate)			
Adequate country under GDPR (EU)			
<b>Blocked until accepted by user:</b> No			
<b>yt-remote-session-name</b>	youtube.com	HTML	Session
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>			
<b>Cookie purpose description:</b> Stores the user's video player preferences using embedded YouTube video			
<b>Initiator:</b> IFrame, page source line number 558			
<b>Source:</b> <a href="https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent">https://www.youtube.com/embed/wx2nbjzhbcc?version=3&amp;theme=dark&amp;color=red&amp;modestbranding=rel=0&amp;showinfo=0&amp;enablejsapi=1&amp;mode=transparent</a>			
<b>Data is sent to:</b> United States (adequate)			
Adequate country under GDPR (EU)			
<b>Blocked until accepted by user:</b> No			

### Category: Unclassified (1)

Unclassified cookies are cookies that we are in the process of classifying, together with the providers of individual cookies.

COOKIE NAME	PROVIDER	TYPE	EXPIRY
<b>style</b>	ufsc.br	HTTP	1 year
<b>First found URL:</b> <a href="https://ufsc.br/">https://ufsc.br/</a>			
<b>Cookie purpose description:</b> Unclassified			
<b>Initiator:</b> Script tag, page source line number 214			
<b>Source:</b> <a href="https://ufsc.br/wp-content/themes/brasilGov/js/functions.js?ver=4.7.16">https://ufsc.br/wp-content/themes/brasilGov/js/functions.js?ver=4.7.16</a>			
<b>Data is sent to:</b> Brazil (not adequate)			

### Unknown subdomains

The following subdomains were discovered but not scanned. Subdomains may also be setting cookies or using similar tracking technologies. Please consider if these subdomains needs to be scanned as well.

- acesso.egestao.ufsc.br
- acessoainformacao.ufsc.br
- agecom.ufsc.br
- apoio pedagogico.prograd.ufsc.br
- ararangua.ufsc.br
- blumenau.ufsc.br
- ca.ufsc.br
- cae.ufsc.br
- cagr.sistemas.ufsc.br
- calouros.ufsc.br
- capg.sistemas.ufsc.br
- cartadeservicos.ufsc.br
- ciencia.ufsc.br
- classificados.inf.ufsc.br
- concursos.ufsc.br
- confere.ufsc.br
- coperve.ufsc.br
- curitiba.ufsc.br
- dae.ufsc.br
- dpqi.seplan.ufsc.br
- editora.paginas.ufsc.br
- egressos.ufsc.br
- estrutura.ufsc.br
- galeria.ufsc.br
- hu.ufsc.br
- identidade.ufsc.br
- inscricoes.ufsc.br
- joinville.ufsc.br
- moodle.ufsc.br

- museu.ufsc.br
- ndi.ufsc.br
- noticias.ufsc.br
- oportunidadesinternacionais.ufsc.br
- ouvidoria.ufsc.br
- pdi.ufsc.br
- periodicos.ufsc.br
- portal.bu.ufsc.br
- portal.estagios.ufsc.br
- portalcds.ufsc.br
- prae.ufsc.br
- proppg.ufsc.br
- repositorio.ufsc.br
- ru.ufsc.br
- saad.ufsc.br
- sapsi.paginas.ufsc.br
- sead.ufsc.br
- secarte.ufsc.br
- segesp.ufsc.br
- servidor.ufsc.br
- sinter.ufsc.br
- sisu2018.ufsc.br
- structure.ufsc.br
- telefones.ufsc.br
- tv.ufsc.br
- vestibular2019.ufsc.br
- vestibularunificado2020.ufsc.br
- webmail.ufsc.br