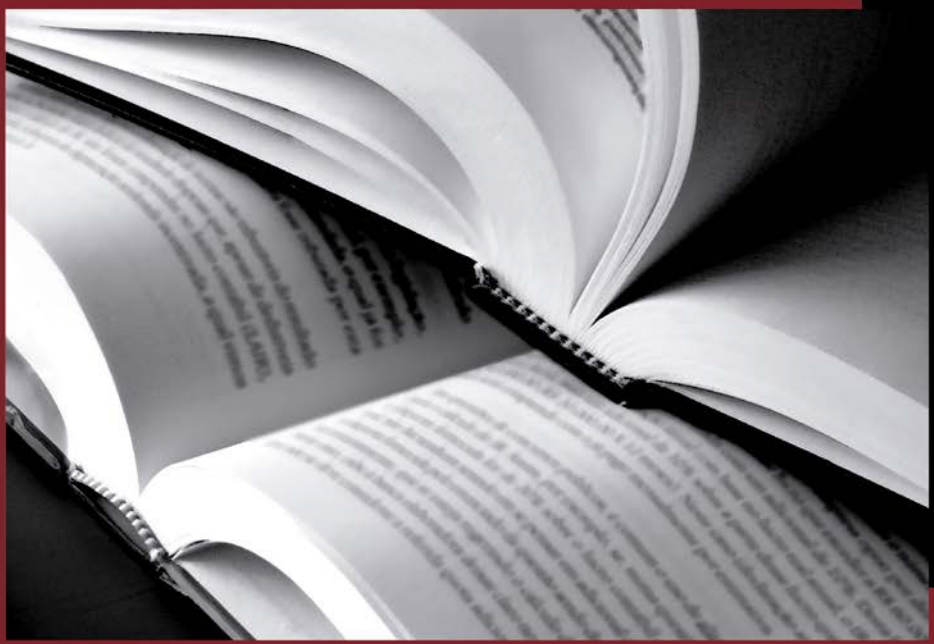
38

SÉRIE MONOGRAFIAS DO CEJ

Lia Carolina Vasconcelos Camurça



Sociedade de vigilância, direito à privacidade e proteção de dados: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário

JUSTIÇA FEDERAL
Conselho da Justiça Federal
Centro de Estudos Judiciários

CONSELHO DA JUSTIÇA FEDERAL

Ministro Humberto Martins
Presidente

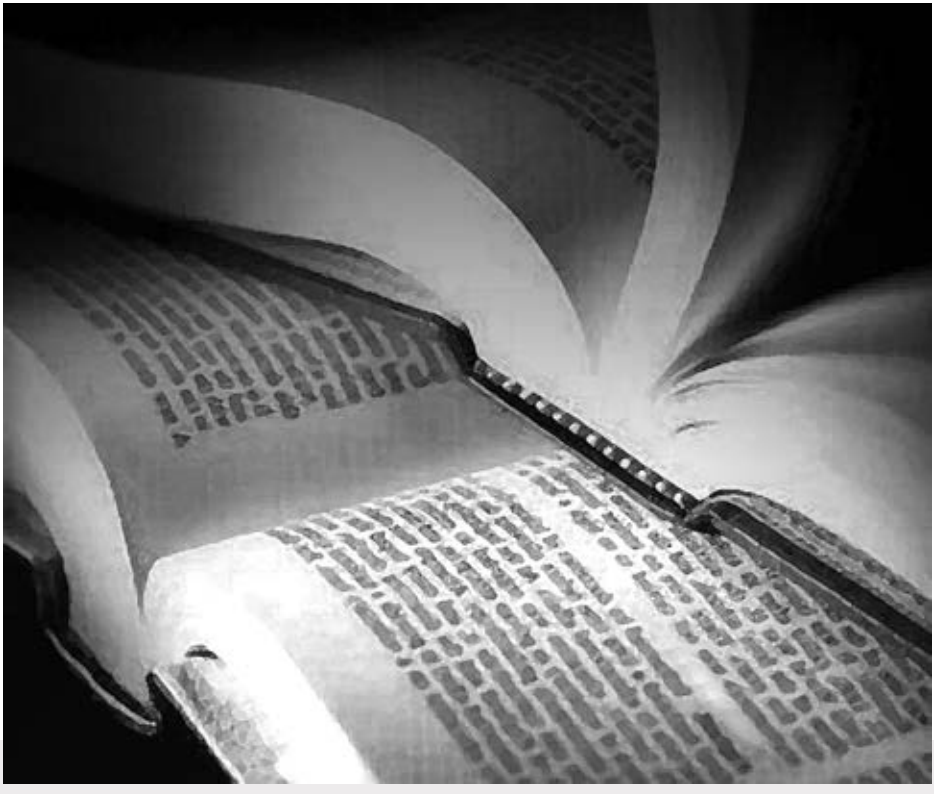
Ministro Jorge Mussi
Corregedor-Geral da Justiça Federal e
Diretor do Centro de Estudos Judiciários

Ministro Villas Bôas Cueva
Ministro Sebastião Alves dos Reis Junior
Ministro Marco Aurélio Gastaldi Buzzi
Desembargador Federal I'talo Mendes
Desembargador Federal Messod Azulay Neto
Desembargador Federal Mairan Maia Júnior
Desembargador Federal Victor Laus
Desembargador Federal Edilson Pereira Nobre Júnior
Membros Efetivos

Ministro Marco Aurélio Bellizze
Ministra Assusete Magalhães
Ministro Sérgio Luíz Kukina
Desembargador Federal Francisco de Assis Betti
Desembargador Federal Guilherme Calmon Nogueira da Gama
Desembargadora Federal Consuelo Yatsuda Moromizato Yoshida
Desembargador Federal Luís Alberto d'Azevedo Aurvalle
Desembargador Federal Alexandre Luna Freire
Membros Suplentes

Juiz Federal Marcio Luiz Coelho de Freitas
Secretário-Geral

SÉRIE MONOGRAFIAS DO CEJ

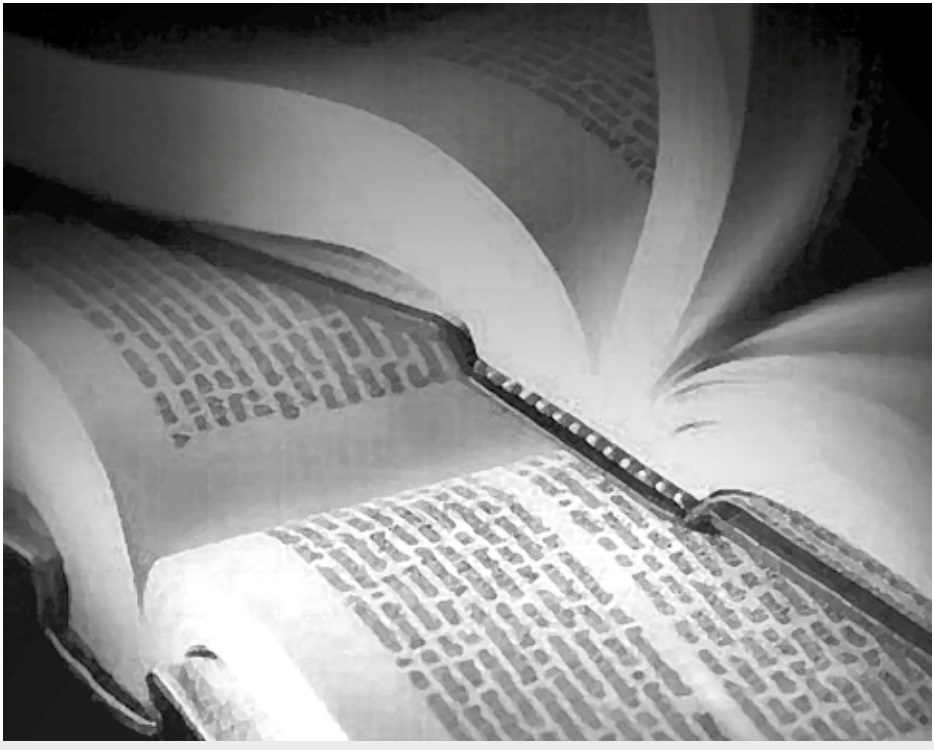


Sociedade de vigilância, direito à privacidade e proteção de dados: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário

Lia Carolina Vasconcelos Camurça

Brasília-DF, junho de 2021 **38**

SÉRIE MONOGRAFIAS DO CEJ



Sociedade de vigilância, direito à privacidade e proteção de dados: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário

Lia Carolina Vasconcelos Camurça

JUSTIÇA FEDERAL
Conselho da Justiça Federal

EDITORAÇÃO
CENTRO DE ESTUDOS JUDICIÁRIOS – CEJ
João Batista Lazzari – Juiz auxiliar da Corregedoria-Geral da Justiça Federal
Deyst Deysther Ferreira de Carvalho Caldas – Secretária

Divisão de Biblioteca e Editoração do CEJ – Dibie/CEJ
Maria Aparecida de Assis Marks – Diretora da Dibie/CEJ
Milra de Lucena Machado Amorim – Chefe da Seção de Editoração da Dibie/CEJ
Helder Marcelo Pereira – Seção de Editoração da Dibie/CEJ (diagramação)
Telma Cristina Ikeda Gondo – Seção de Editoração do CEJ da Dibie/CEJ
Ana Paula Lucena Silva Candeas – Seção de Editoração da Dibie/CEJ

C211s Camurça, Lia Carolina Vasconcelos.
Sociedade de vigilância, direito à privacidade e proteção de dados pessoais : uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário / Lia Carolina Vasconcelos Camurça. – Brasília : Conselho da Justiça Federal, Centro de Estudos Judiciários, 2021.
279 p. – (Série Monografias do CEJ ; n. 38).

1. Proteção de dados pessoais. 2. Direito à privacidade. 3. Internet, aspectos jurídicos. 4. Consumidor, aspectos psicológicos. 5. Proteção e defesa do consumidor. 6. Publicidade subliminar. 7. Inteligência artificial, aspectos jurídicos. I. Série.

CDU 342.721

Ficha catalográfica elaborada por Lara Pinheiro Fernandes do Prado – CRB 1/1254

A todos que se sentem vigiados no mundo digital..

AGRADECIMENTOS

Difícil a missão de elencar agradecimentos após esses dois anos intensos, fisicamente e psicologicamente. Inicio, assim, agradecendo àqueles que pavimentaram o caminho para que eu chegasse a este momento. Agradeço à minha amada mãe, Claudia, pois sem ela, literalmente, não estaria aqui, tanto porque me carregou em seu ventre, quanto bem porque, em sua autoridade materna, não me deixou desistir de realizar a prova de seleção do mestrado, apesar de minhas inseguranças. Os seus olhos verdes de menina, que sempre me olham com tanto orgulho, motivam-me a não desistir dos meus sonhos. Ao meu pai, Irapuan, pelo carinho constante e por me inspirar a trilhar este caminho do Direito, além de sempre ter apoiado de todas as formas o meu aprimoramento como mulher e profissional. Aos meus avós Maria e Epifânio, pelos ensinamentos de infância que estarão para sempre gravados em meu caráter. Às minhas tias Ana, Fernanda e Maciene, por serem parte da minha pequena e feliz família. À Serena, pelo amor incondicional. Serei eternamente grata ao PPGD/UFC, por me aproximar da minha tia Eulália, cuja convivência é um tesouro, por possuir sempre as palavras sábias e inspiradoras na voz mais doce, como: "Não fique nervosa, o nervosismo é sinal de arrogância, não há trabalho corretíssimo e completo o bastante que não receba críticas". Ao Bruno, pelo companheirismo e paciência, por ser incessável fonte de conhecimento histórico da humanidade, bem como pela sincera e crítica r
evisão deste trabalho.

Agradeço especialmente ao professor João Luís pela paciência que despendeu em mais uma orientação e por ter sido um grande mestre desde a minha graduação, guiando-me como aluna, monitora, bolsista e mestranda. Ao professor André Dias, por gentilmente ter contribuído com a evolução deste trabalho desde a qualificação, cujas críticas foram essenciais para o desenvolvimento de argumentos presentes nesta versão final. Ao professor George Marmelstein, por ter aceito o presente

convite, bem como por me motivar, por meios de seus posts e palestras, a configurar a mente para uma super aprendizagem.

Aos meus queridos amigos de infância, adolescência e vida adulta, que felizmente tenho a sorte de dizer que são consideráveis, pelo apoio e pela confiança em mais esta etapa da minha vida. Também agradeço aos meus colegas do PPGD/UFC, que, apesar da minha reserva e timidez, dispuseram-se a compartilhar comigo suas experiências e conhecimentos de vida.

Agradeço aos funcionários das bibliotecas da Faculdade de Direito (BFD), do campus do Pici Prof. Francisco José de Abreu Matos (BCCP) e de Ciências Humanas (BCH), pela paciência, apesar de eu ter perdido um livro (posteriormente encontrado), e por manterem, na medida do possível, a qualidade do acervo que foi amplamente utilizado neste trabalho.

Ao professor Danilo Doneda, por gentilmente enviar cópia de seu livro, referencial teórico na matéria, apesar de esgotado em todas as livrarias do Brasil.

Agradeço à Universidade Federal do Ceará, por proporcionar meus estudos de graduação e pós-graduação de forma totalmente gratuita, o que me motiva a devolver à sociedade o conhecimento que obtive neste ambiente público.

Por fim, agradeço à Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico (FUNCAP), pela concessão de bolsa de estudo, a partir de março de 2019, como apoio financeiro ao desenvolvimento científico.

"Are we not all prisoners? She had read a wonderful play about a man who scratched on the wall of his cell, and she had felt that was true of life – one scratched on the wall." (Virginia Woolf *em* Mrs. Dalloway)

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados Pessoais
CDC	Código de Defesa do Consumidor
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
DNT	Do Not Track
DPDC	Departamento de Proteção e Defesa do Consumidor
DPIA	Data Protection Impact Assessment
EUA	Estados Unidos da América
FIPPs	Fair Information Practice Principles
FTC	Federal Trade Comission
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IA	Inteligência Artificial
IBM	International Business Machines Corporation
ico.	Information Commissioner's Office
IDEC	Instituto de Defesa do Consumidor
IoT	Internet of Things
LGPD	Lei Geral de Proteção de Dados Pessoais
LIA	Legitimate Interests Assessment
NAI	Network Advertising Initiative
OBA	Online Behavioral Advertising
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMC	Organização Mundial do Comércio

P3P	Platform for Privacy Preferences
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
RIPD	Relatório de Impacto à Proteção de Dados
RGPR	Regulamento Geral de Proteção de Dados Pessoais
SENACON	Secretaria Nacional do Consumidor
STJ	Superior Tribunal de Justiça
W3C	World Wide Web Consortium

LISTA DE ILUSTRAÇÕES

SOBRE A AUTORA

Lia Carolina Vasconcelos Camurça é Advogada. Mestra em Direito Constitucional pelo Programa de Pós-graduação em Direito pela Universidade Federal do Ceará – UFC (2020). Ex-bolsista da Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico. Pesquisadora na área de Direito, com foco em Direito Civil e em Direito Comercial.

SUMÁRIO

1 Introdução

O detentor de informações – sobre si mesmo, clientes, concorrentes ou Estados – possui grande poder, no sentido mais sutil da palavra, qual seja, o da possibilidade. Esta possibilidade de criar padrões, inspirar desejos ou sobressair-se no mercado faz com que as informações, mais precisamente os dados, tornem-se moeda de grande importância na economia.

Nunca os dados pessoais estiveram em ampla discussão na sociedade brasileira. A matéria da proteção de dados pessoais está sendo amplamente discutida nos mais diversos âmbitos sociais, como em lançamentos de obras nacionais, discussões em grandes veículos da mídia e até mesmo com a publicação de vídeos institucionais no YouTube.

Assim, cada vez mais a proteção de dados

pessoais se torna um tema atual e relevante no Brasil. Segundo o *Google Trends* – ferramenta do *Google* que permite acompanhar a evolução das buscas por certo termo ou palavra-chave – a procura pelo tema "proteção de dados" saiu de 0,02% de pontos de interesse dos usuários em março de 2015 para 100% de interesse dos usuários em agosto de 2018.[1] Ou seja, um aumento de quase 500% de interesse do público brasileiro pelo assunto.[2]

A promulgação da Lei Geral de Proteção de Dados Pessoais, doravante chamada de LGPD e Lei Geral, foi um dos vetores para o fortalecimento da discussão. Contudo, o presente trabalho não é fruto da discussão nascida com a promulgação da lei, posto que, como os aspectos inerentes a uma legislação, ele ficaria defasado em questão de meses ou dias.

Em verdade, o questionamento principal deste estudo surgiu de uma inquietação em sala de aula: até que ponto a vigilância dos usuários na internet, realizada por entes privados, é atentatória ao direito à privacidade e põe em risco a autodeterminação humana?

O indivíduo que decidir escolher por uma privacidade máxima e restrita para si próprio pode encerrar-se em ostracismo, eis que, hoje, para se conectar minimamente, deve renunciar a informações pessoais mínimas, tais como nome, documentos pessoais e endereço de IP. Este é preço de incluir-se na sociedade digital.

Tal preço, contudo, não é percebido por grande parte dos indivíduos, que sequer notam que o fornecimento de dados como o CPF, o RG e o *e-mail* são de grande valia para o comércio físico e eletrônico. A ideia de que, enquanto cidadão, não se tem nada a esconder ou que a sua vida privada não é interessante a ponto de ter seus dados coletados revela a ausência da compreensão, pelas pessoas, da preciosidade dos dados pessoais nos novos modelos de negócios digitais.

Investigar os limites da privacidade na era dos novos negócios digitais, em que as técnicas de monitoramento do usuário são parte essencial da movimentação econômica e personalização da experiência *on-line*, re-

1 Mês de promulgação da Lei Geral de Proteção de Dados Pessoais.

2 Pesquisa pelo termo "proteção de dados" no Google Trends. Disponível em: <https://trends.google.com.br /trends/explore?date=today%205-y&geo=BR&q=prote%C3%A7%C3%A3o%20 de%20dados>. Acesso em: 6 jan. 2020.

velam reflexos na capacidade de decisão e escolha do cidadão.

Apesar da importância dos dados para o comércio, o valor para o fornecimento de informações pelo usuário é ínfimo, por vezes consistindo em mero cadastro para ganhos de descontos, ou até mesmo a mera juntada de pontuações em estabelecimentos. É possível comparar a ausência de conscientização do que se faz com os dados pessoais dos cidadãos ao não se saber a diferença de valor entre uma nota de dois reais (dar a informação por descontos) e uma nota de cem reais (receber a informação e tratá-la consoante quaisquer parâmetros).

Enquanto para o fornecedor cidadão o incômodo de fornecer a informação é ínfimo para obter um benefício supostamente maior, para aqueles que a recebem e sabem utilizá-la, ela é transformada para muito além do que receberam, podendo enquadrá-la em perfis comportamentais. Com isso, de forma invisível, mas curiosamente sem transparência, sustentam-se reinados dos detentores da informação, que além da simples posse possuem a possibilidade de tratá-la de mais variadas formas, sem limite aparente de armazenamento, graças ao *big data*.

Os grandes vazamentos de dados pessoais ocorridos nos últimos anos também reforçam a problemática que os danos gerados por tal prática, por vezes, são irreparáveis ante as características inerentes ao mundo digital.

Assim, um paradoxo surge na problemática principal: se a informação é volitivamente entregue pelo indivíduo, como isto poderia se configurar uma ameaça à privacidade? O julgamento dos cidadãos sobre a validade de ganhar descontos ou bônus pela rápida entrega de números estaria prejudicado sob quais razões?

Muito além de buscar interferir na possibilidade de as pessoas fornecerem seus dados por quaisquer valores, a partir do momento que estes são tratados, a forma que se utiliza o tratamento implica em consequências que vão além do usuário fornecedor dos dados. Além disso, é indispensável verificar que, por vezes, após a formação dos bancos de dados, a depender da legislação protetiva ou até mesmo se o usuário, sem perceber, autorizou seu reenvio a outros países, pode-se criar perfis comportamentais de milhares de usuários, passando a se enquadrar em pessoas que sequer consentiram com esta análise.

Assim, pelos motivos elencados, justifica-se a relevância da temática

objeto de análise do presente estudo acadêmico. A pergunta que delineia o capítulo inicial é: quais são as novas feições do direito à privacidade relacionadas ao eixo constitucional da proteção da pessoa?

Neste capítulo abordou-se que a privacidade é um conceito que vai se redesenhando ao longo do tempo. Surgido nos Estados Unidos como o direito de ser deixado só, evoluiu, na atualidade, para o direito do resguardo do indivíduo contra interferências alheias, ou seja, o poder de revelar-se seletivamente ao mundo.

Essa revelação seletiva ao mundo pode parecer simples, contudo, a partir do momento em que o homem se insere no ambiente digital, suas informações são disseminadas de forma quase incontrolável. Por exemplo, por meio da ferramenta do *Google Street View*, descobriu-se uma traição, apesar dos rostos e placas serem borrados no sistema de visualização de ruas. O formato corporal e roupas foram dados pessoais com potencial identificador suficiente para a identificação de um indivíduo.[3]

No mundo de reinados tecnológicos invisíveis, muitas vezes a proteção da privacidade é vendida como um diferencial no mercado capaz de tornar uma empresa mais competitiva ou não.

Aborda-se outra expressão do direito à privacidade, qual seja, o direito à autodeterminação informativa, passando ao centro das discussões da proteção da privacidade *on-line*. Surgido de uma reivindicação da autonomia do indivíduo na sociedade de informação, a decisão histórica da Corte Constitucional Alemã, comentada no capítulo 2, consagrou referido direito em 1983. Este transpassa o direito de o indivíduo controlar sua intimidade e vida privada ao direito de possuir controle sobre a informação que lhe diz respeito retida por outros.

Ainda no mesmo capítulo analisa-se a indagação: quais são os desdobramentos do consentimento no ambiente digital? Como principal consequência do consentimento está a ocorrência de um superdimensionamento deste em que, partindo de um pseudoconsentimento, obtêm-se permissões por entes privados para o profundo conhecimento de alguém

3 HOHMAN, Maura. Man Divorces Wife After Accidentally Catching Her Cheating on Google Maps Street View. People. 2018. Disponível em: <https://people.com/home/man-catches-wife-cheating-google-maps-street-view-they-divorce/> Acesso em: 5 jan. 2020.

e, consequentemente, podem se tornar intromissões de cunho comportamental na vida do usuário.

Armas lícitas podem se converter em armas envenenadas se utilizadas de maneiras inapropriadas. Com isso, o capítulo 3 foca na publicidade comportamental e nas práticas para a coleta de dados *on-line*, partindo da pergunta: quais são as práticas mais comuns e as consequências da sua utilização para obtenção de dados para direcionamento de publicidade nos novos modelos de comércio eletrônico?

Assim, escolheu-se analisar as ferramentas de *cookies*, *web beacons*, *supercookies,* HTML5 *web storage* e *fingerprinting*, pela escassez da análise destas em trabalhos em português e no ramo do Direito. As ferramentas acima foram selecionadas entre outras existentes por serem as mais recorrentes nas análises da bibliografia estrangeira analisada pela autora, especificamente a referenciada no capítulo 3.

Analisadas em ordem crescente de prejudicialidade ao usuário, as práticas podem se iniciar desde a instalação de *cookies* – que partem de uma permissão ativa do usuário – até a realização de *fingerprinting*, a técnica mais invasiva citada pelos estudos analisados, que permite o rastreamento persistente do indivíduo.

Após estas análises teóricas, passou-se ao estudo prático de situações de criação de perfis comportamentais de usuários na internet, com destaque aos casos paradigmáticos com demasiados riscos de manipulação de dados para *profiling*, bem como riscos à privacidade dos usuários. Optou-se por excluir o célebre caso do direcionamento de publicidade política da *Cambridge Analytica*, por não envolver diretamente serviços direcionados unicamente aos consumidores.

Por fim, no último capítulo, analisam-se as perspectivas da Lei Geral de Proteção de Dados Pessoais, partindo do histórico e do contexto social e econômico da promulgação da lei. Notando que a Lei Geral regulou tratamento de dados pessoais desde a coleta ao descarte, incluindo o mero armazenamento, indagou-se: A LGPD é capaz de colocar o Brasil em patamar para realização de transações internacionais de dados pessoais?

Para obter a resposta desta indagação, analisou-se as características do consumidor europeu em relação ao consumidor brasileiro, abrangendo temas como a existência do direito à explicação de decisões automati-

zadas, a efetividade da atuação da Autoridade Nacional de Proteção de Dados, bem como a tentativa de uma mudança da centralidade do consentimento a partir da criação de diversas bases legais.

Entre as conclusões do trabalho estão que ambientes geridos unicamente por algoritmos dificultam a proteção da privacidade. A tecnologia pode ser forte vetor de variadas formas de manipulação, já que a sua escolha pode restringir ou anular por completo a atuação jurídica – como exemplo, as decisões judiciais de reiterados bloqueios em vão do aplicativo *WhatsApp*, que adota criptografia de ponta a ponta.

Uma Lei Geral de Proteção de Dados, por si, só não é capaz de resolver todos os problemas inerentes à utilização de dados pessoais no ambiente digital, não enquanto o domínio e a manipulação da tecnologia sejam indiscriminadamente decididos pelos agentes econômicos.

No presente trabalho, buscou-se evitar anglicismos, observando a crítica de Newton de Lucca de que a utilização impensada de termos estrangeiros significa "um verdadeiro abuso de barbarismos injustificáveis, como se dessa tecnolinguagem alienígena tivesse algo a ver com erudição científica" (LUCCA, 2005, p. 34). Os estrangeirismos que foram mantidos são aqueles já incorporados à língua portuguesa como: internet, *on-line*, *marketing* e interface. Ademais, foram mantidos aqueles que, por serem pouco utilizados em doutrinas em português, acabam por não possuir uma tradução fiel ao seu conteúdo, como: *profiling*, *data mining* e *trade off*. Optou-se por deixar o nome de marcas sem o destaque em itálico, mesmo que estrangeiras, haja vista sua grande penetração no cotidiano.

Os termos que se referem à sociedade foram réplicas daqueles mais utilizados na bibliografia específica, como sociedade de informação, sociedade de vigilância[4], sociedade interconectada, sociedade pós-moderna e sociedade líquida[5], mas significam todas as sociedades contemporâneas (FERNANDES, 2015, p. 43).

4 Termo criado por Stefano Rodotà em seu livro *A vida na sociedade de vigilância: A privacidade hoje*, que discute o direito à privacidade nas relações sociais vigiadas pelo Estado e pelos outros indivíduos.

5 Termo do sociólogo Zygmunt Bauman, que trata da liquidez das relações humanas em diversas obras.

Por fim, a estruturação das referências bibliográficas em tópicos, agrupando os tipos de referência correlatas, foi realizada a partir do exemplo da obra de Bruno Bioni, *Proteção de Dados Pessoais: a função e os limites do consentimento*.

Adotou-se como metodologia, principalmente, a pesquisa bibliográfica. Foi feita, inicialmente, a exploração de fontes bibliográficas tais como livros, teses, dissertações, monografias, artigos científicos, sites governamentais e institucionais, entre outros. As bibliotecas da Universidade Federal do Ceará foram, juntamente com pesquisas em sítios na internet, os principais acervos do projeto.

Feito isso, houve uma ordenação das informações obtidas, de acordo com seu conteúdo, e a posterior análise dos dados. Assim, a pesquisa é de natureza bibliográfica, exploratória, descritiva e interpretativa, de cunho qualitativo, mediante análise doutrinária e documental.

Vale destacar que este trabalho opta pela análise dos efeitos da interação de empresas privadas com o tratamento de dados pessoais de indivíduos, bem como a capacidade de moldar comportamentos humanos partindo de análises de dados por entes privados. Este recorte faz-se necessário para uma avaliação mais criteriosa das particularidades dessa interação, de forma a tentar obter maior precisão nas conclusões apresentadas.

No entanto, são brevemente comentados casos de interação pública com os dados pessoais, já que esta interação foi o que deu ao tema as suas origens e a importância que possui hoje.

2 A sociedade de vigilância de dados pessoais

Neste capítulo inicial, tratar-se-á dos contornos do direito à privacidade e da formação do consentimento na atual sociedade de informação. O poder vinculado à informação, nas últimas décadas, delineou de forma surpreendente a interação social no mercado econômico em que ela se insere e em suas demandas. A informação transforma o homem, definindo-o, classificando-o e etiquetando-o.

A informação se mostra cada vez mais valiosa e poderosa, pautando verdadeiramente a economia atual. A economia dos dados – *data economy* – possibilitou que negócios aparentemente gratuitos, como as mídias sociais, possam movimentar milhões de dólares sem que a maioria da população se dê conta de que esta moneti-

zação provém das informações que cada indivíduo fornece volitivamente – ademais, por vezes, em contexto não volitivo, já que o consentimento no século XXI cada vez mais está se resumindo a um clique na cláusula final dos contratos de adesão, disfarçados de "Termos de Uso", geralmente chamada de "Li e Aceito".

Nesse contexto, sobressai-se a transformação da tutela da privacidade, destacando-se que a sua proteção e seu resguardo está verdadeiramente fora de moda. Com isso, tal direito, a princípio, costuma ser olvidado como direito fundamental, ou até mesmo ter sua eficácia posta em dúvida. Por exemplo, no Brasil, sua única menção no Título II da Constituição Federal, dos Direitos e Garantias Fundamentais, se dá por meio do genérico termo "vida privada". Mundo afora, a proteção à privacidade enfrenta obstáculos impostos pelo próprio Estado, a título de monitoramento de cidadãos ou até de segurança nacional, passando a ser vista não como direito fundamental, mas sim como obstáculo à segurança (RODOTÀ, 2008, p. 14).

Partindo desses pressupostos, o presente capítulo foi organizado em quatro tópicos, iniciando com a análise dos reinados invisíveis empresariais a partir da transformação do ser humano em informação na sociedade de vigilância; analisando, em seguida, a reinvenção do direito à privacidade na atualidade; evidenciando, ainda, a construção do direito à autodeterminação informativa. Trata-se, ainda da usurpação do consentimento, principalmente quanto ao alcance jurídico das cláusulas de "Li e Aceito", o que conduz ao encerramento da seção, com a análise dos termos de uso sob a ótica consumerista.

2.1 A sociedade de vigilância: reinados tecnológicos invisíveis

A chamada globalização já se consolidou no cotidiano e transforma a sociedade em um ritmo jamais visto. A própria internet se transforma velozmente, integrando-se com o homem de forma sequer pensada na ficção. Mark Weiser já ditava, em 1999, que as tecnologias mais profundas eram aquelas que desapareciam no dia a dia, até se

tornarem indistinguíveis da rotina.[6] A ilusão de grandes aparatos robóticos em uma sociedade futurista se dissipa nas tecnologias cada vez mais pensadas para serem invisíveis.

No mesmo sentido, o economista Joseph Schumpeter, um dos primeiros a considerar a inovação tecnológica em nosso tempo, chama de destruição criadora, chave para a compreensão do capitalismo, a "[...] mutação industrial [...] que revoluciona incessantemente a estrutura econômica a partir de dentro, destruindo incessantemente o antigo e criando elementos novos. Esse processo de destruição criadora é básico para se entender o capitalismo".[7]

Essa disrupção criativa que favorece um ambiente de mudança tecnológica efetivamente foi posta em prática, tanto que o termo inovação disruptiva virou clássico em debates de empreendedorismo.

Contudo, permite-se apontar que a maior inovação disruptiva dos últimos anos foi a criação de um plano de negócio que partisse de um insumo extremamente valioso e facilmente coletável: a informação. Os maiores modelos de negócios da atualidade giram em torno da monetização dos dados, potencializados pelo valor que eles possuem. Assim, o *trade off*[8] do compartilhamento dos dados, em detrimento do direito à privacidade do usuário, é alto.

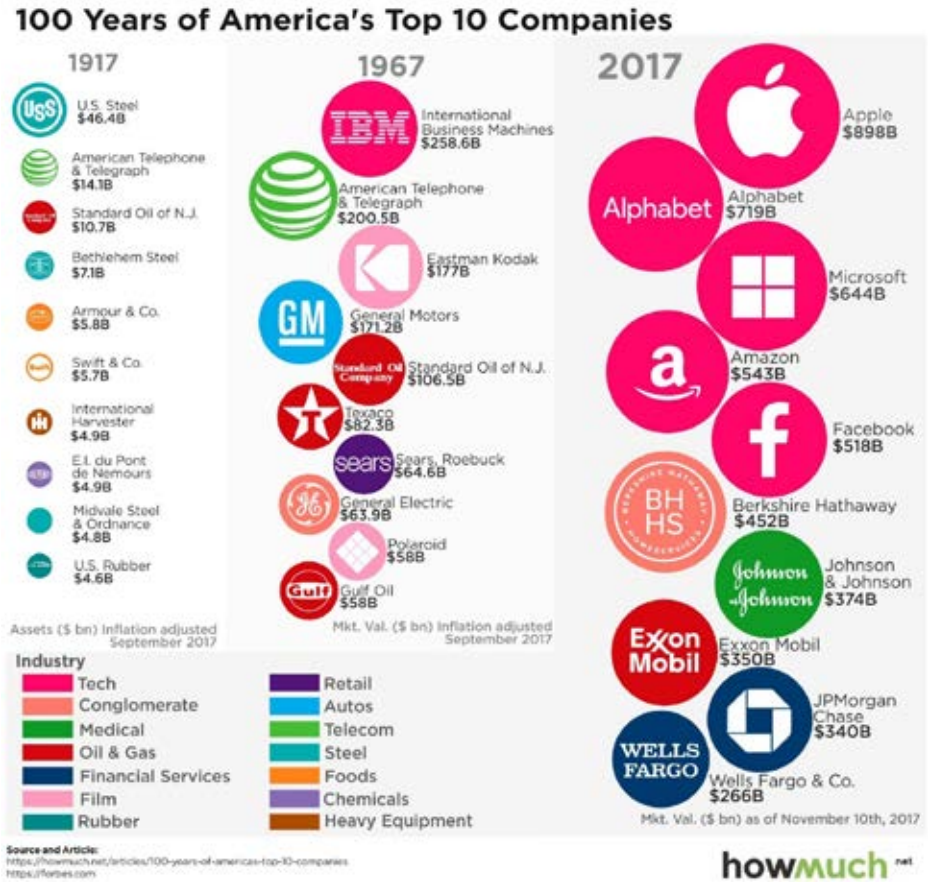
Assim, destaca-se um gráfico de análise de dados da revista *Forbes* indicando as maiores companhias dos Estados Unidos em 1917, 1967 e 2017.

6 WEISER, Mark. The Computer for the 21st Century. **SIGMOBILE Mob**. Rev. 3, July, 1999. p. 3-11. Doi: http://dx.doi.org/10.1145/329124.329126. p. 1. Disponível em: <https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf> Acesso em: 25 nov. 2018.

7 Tradução livre. Original: "[...] *industrial mutation* [...] *that incessantly revolutionizes the economic structure from within, incessantly destroying the old one, incessantly creating a new one*" (SCHUMPETER, 2003. p. 83).

8 Conceito da Economia que se preferiu não traduzir, por abarcar amplo espectro de definições em português, mas utilizado no presente texto no sentido da vantagem da escolha de uma coisa em detrimento de outra.

FIGURA 1 – CEM ANOS DAS TOP 10 COMPANHIAS DOS ESTADOS UNIDOS DA AMÉRICA

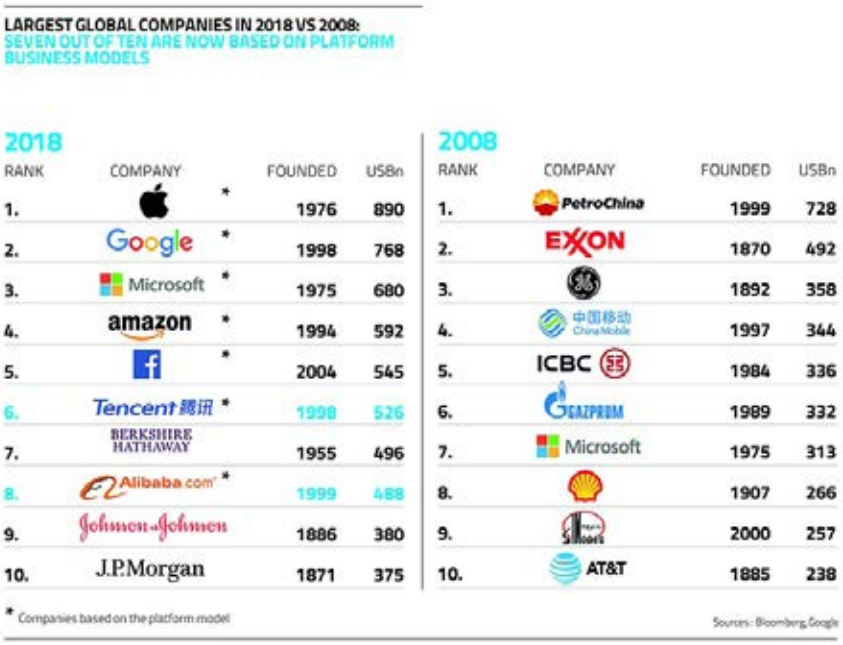


Fonte: AMOROS, Raul. A Century of America's Top 10 Companies, in One Chart. *Howmuch.net*. 2017. Disponível em: <http://tiny.cc/ojdf8y>. Acesso em: 17 jun. 2019.

Nota-se que a percursora de uma economia de dados, a *International Business Machines* (IBM) – sequer constante na lista em 1917, apesar de já criada em 1911 – já desponta, em 1967, como a maior companhia dos Estados Unidos, acompanhada por empresas de petróleo ou de motorização. Em 2017, porém, o panorama mudou drasticamente, sendo as cinco primeiras empresas da lista fortemente relacionadas a economia de dados.

Relevante, ainda, a análise global das maiores companhias do mundo por valor, comparadas no espaço temporal de 2008 a 2018:

FIGURA 2 – MAIORES COMPANHIAS GLOBAIS EM 2018 VS. 2008[9]



Fonte: SCHENKER, Jennifer. The Platform Economy. *The innovator*. 2019. Disponível em: <http://tiny.cc/zkdf8y> Acesso em: 17 jun. 2019.

Mais uma vez, percebe-se a drástica mudança nas maiores atividades econômicas exercidas globalmente, que se transacionaram da exploração dos recursos naturais para o aproveitamento do capital imaterial. Na análise global, sete[10] das dez listadas são empresas que possuem como sua base a monetização de dados.

A maior companhia global e americana, nos dois gráficos, é a *Apple*. Shoshana Zuboff credita isso ao *Apple Hack*, isto é, à forma como a empre-

9 Destaque-se, brevemente, a discordância em relação ao autor da figura quanto à posição n. 2, eis que estaria mais corretamente denominada de Alphabet, a empresa controladora do Google.

10 *Apple, Alphabet, Microsoft, Amazon, Facebook, Tencent* (comparado a um Facebook chinês) e *Alibaba*.

sa *hackeou* os consumidores para serem ávidos aos seus lançamentos. Em que pese a lógica da linha de produção fordista ser revolucionária, ela proporcionava pouca chance de personalização pelo usuário – exemplo disso é a clássica máxima de Henry Ford: "Você pode ter um carro de qualquer cor, desde que seja preto". Por sua vez, a *Apple* reescreveu a interação consumerista, colocando o poder de personalização de cores e visualização do sistema nas mãos dos consumidores, destacando-se com seu design inovador e marketing genioso. A autora afirma, ainda, que a empresa gerou mais lucro para seus investidores do que qualquer outra companhia americana no século XX (ZUBOFF, 2019).

Com isso, vale destacar que "[...] a arma dos tempos modernos não é a bomba, mas a informação. Quem detém a informação tem o poder" (GUERRA, 2004, p. 1).

Muito se utiliza a palavra impacto para designar a força do mundo conectado na sociedade. Contudo, esse impacto já está há muito tempo defasado, não havendo mais motivo para se falar em impacto da tecnologia na sociedade. Para o filósofo Pierre Lévy (2010, p. 21), falar em impacto seria comparar a tecnologia a um projétil com um alvo determinado, não sendo tal metáfora correta para tratar das tecnologias. Em suas palavras: "Em vez de enfatizar o impacto das tecnologias, poderíamos igualmente pensar que as tecnologias são produtos de uma sociedade e de uma cultura" (LÉVY, 2010, p. 22). Essa cultura, que se altera cada vez mais rápido, produz, em vez de impacto, insegurança nas relações.

A proteção da privacidade na relação entre o cidadão e o Estado, apesar de muito pertinente no contexto moderno, foge aos objetivos do presente trabalho, que buscou destacar as interações do direito à privacidade dos cidadãos aos ataques com fins de mercado. Contudo, não se pode deixar de mencionar o *USA Patriot Act*, decreto americano que serviu como resposta aos atentados terroristas de 11 de setembro de 2001, que foi, em verdade, um verdadeiro atentado à privacidade de cidadãos americanos e de mais diversas nacionalidades. Além disso, há o exemplo do *Etat d'urgence* na França, com medidas excessivamente restritivas, postas em práticas inicialmente com os ataques ao jornal satírico *Charlie Hebdo*, que em vez de durar os iniciais dozes dias, foram sucessivamente prorrogadas por dois anos.

Os ataques cibernéticos se tornaram preocupação constante nos governos hodiernos. A dependência dos homens em relação às máquinas aumenta cada vez mais, transmutando-se em uma dependência da informação, válvula do poderio econômico. Nas palavras de Túlio Vianna (2007, p.46):

> A informação é o meio de produção da própria informação e, na economia pós-industrial, é também o produto de maior valor. Toda a economia está voltada prioritariamente para a produção de mais informação e o poder de dominação é exercido pelos detentores dos mais diversos tipos de informação: tecnológica, nuclear, publicitária, cultural, etc. **A informação tornou-se o mais poderoso instrumento para subjugar a espécie humana** (grifos nossos).

A informação, além dos dados, indica o conhecimento profundo do ser humano. O acesso ao *big data* – tão conhecido e, ao mesmo tempo, de difícil definição – por si só, não leva a um grande poderio econômico. Ou seja, apenas deter dados não configura grande poder caso não se possua a capacidade de transformar esses dados em informação útil e desejável.

Os dados, devidamente analisados, têm a potencialidade de identificar uma pessoa, partindo de seu perfil social, seus hábitos e preferências e seu histórico de transações. Assim, engloba-se a noção de dados pessoais. Os dados são fenômenos da faceta da personalidade da pessoa. Vale destacar que esse fenômeno não se dá apenas com as novas legislações e regulações emergentes no mundo sobre dados, mas, a exemplo da normatividade brasileira, já se encontravam os dados como identidade no art. 21 do Código Civil[11]; dados como desenvolvimento da personalidade no art. 11 do mesmo código[12]; e os dados como privacidade no art. 5º, incisos V e X da Constituição Federal.[13]

11 Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

12 Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

13 Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-

Assim, esse mundo conectado, para além de globalizado, tornou-se vigiado. O capitalismo de vigilância, conceito criado por Shoshana Zuboff, está imune às tradicionais reciprocidades que se formaram entre as populações para a geração de empregos e de consumo, já que a população é alvo de coleta massiva de dados.[14] A vigilância ocorre também pelas grandes empresas de tecnologia, que de forma a obscurecer cada vez mais o controle dos usuários, obscurecem suas operações. Seus atos são quase indetectáveis, e isto ocorre posto que a rapidez com que o *big data* transformou a vida social não acompanhou a rapidez do Direito em tutelar a tecnologia.

A sociedade da informação se identifica como a sociedade de serviços, uma vez que quanto maior a sofisticação tecnológica destes, mais o cidadão fica à mercê do provedor de serviços, por reterem seus dados pessoais. Na explicação de Stefano Rodotà (2008, p. 100):

> A opção, nesse ponto, é aquela notória entre a aceitação incondicional da lógica de mercado e a criação de um quadro institucional caracterizado pela imposição de formas de tutela das informações pessoais; entre direito à privacidade como limite ao jogo espontâneo das forças e **direito à privacidade como mera distribuição de títulos de propriedade livremente negociáveis no mercado** [grifo nosso].

Esta afirmação sintetiza cruelmente o que ocorre nas últimas décadas com o direito à privacidade. Mas será que ele seria tão negociável assim? Por vezes, a negativa em tratar o direito à privacidade como um título negociável pode gerar a exclusão social do indivíduo que não aceita compartilhar seus dados com certas empresas ou provedores de aplicação.

-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] V – é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; [...] X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

14 ZUBOFF, Shoshana. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal Of Information Technology**, [s.l.], v. 30, n. 1. p.75-89, mar. 201. p. 86. SAGE Publications. http://dx.doi.org/10.1057/jit.2015.5. Disponível em: <https://papers.ssrn.com/sol3/papers.c fm?abstract_id=2594754>. Acesso em: 14 mar. 2019.

A título de exemplo, um funcionário de certo escritório não concorda com os "Termos e Política de Privacidade" do aplicativo *WhatsApp*. Em seu direito, não utiliza a aplicação para proteção da sua intimidade e vida privada, já que acredita que tal política, além de pouco acessível (posto que, apesar de possuir milhares de usuários brasileiros, o aplicativo está com seção de privacidade em inglês), sabe que ela se utiliza do método de *cookies*: "[...] [o] *WhatsApp* poderá transferir dados dentro da grupo de empresas do Facebook e para terceiros, incluindo provedores de serviços e outros parceiros".[15] Contudo, as discussões sobre o trabalho e a divisão das tarefas deste funcionário, por certo período que o chefe esteja realizando visitas *in loco*, dar-se-iam apenas por meio do aplicativo. Esta situação pode gerar grande desconforto no ambiente de trabalho se tal funcionário continuar se negando a acessar a aplicação.

Outro exemplo é que certa pessoa, ao descobrir que o emprego dos sonhos em outro país está selecionando candidatos em todo o mundo e a entrevista se dará por meio *software Skype.* Esta pessoa, no caso, discorda da política de privacidade do *Skype*, que é a mesma política da *Microsoft*, que prevê a coleta "interações, uso e experiências com nossos produtos" e que:

> Quando pedimos que forneça os seus dados pessoais, você pode recusar. Muitos dos nossos produtos exigem alguns dados pessoais para que o serviço seja oferecido. **Caso você opte por não disponibilizar os dados necessários para o fornecimento de um produto ou recurso, você não poderá usá-lo**. [...][16]

Nisto, não havendo qualquer flexibilização de tal política de privacidade, o indivíduo terá que decidir se compartilhará seus dados, renunciando

15 Tradução livre: "*WhatsApp may transfer data within the Facebook family of companies and to third parties, including service providers and other partners*".. WHATSAPP. **Informação Legal do Whatsapp**. Disponível em: <https://www.whatsapp.com/legal/?lang=pt_br#privacy-shield> Acesso em: 29 mai. 2019.

16 Política de Privacidade da *Microsoft*. Consta-se, ainda, que os dados serão utilizados para "Anunciar e comercializar para você, incluindo o envio de comunicações promocionais, o **direcionamento de anúncios** e a apresentação de ofertas relevantes para você". [grifos nossos]. MICROSOFT. **Política de Privacidade da Microsoft**. Disponível em: <https://privacy.microsoft.com/pt-br/privacystatement/> Acesso em: 12 mar. 2019.

à sua privacidade e participando da entrevista, ou desistir da seleção.

Tais exemplos podem se replicar em muitos dos provedores de aplicação atuais, em que, por ser inexistente qualquer flexibilização da política de privacidade, a escolha será aceitar os termos integralmente ou não utilizar a aplicação. Partindo de uma análise superficial, poder-se-ia pensar que não gera quaisquer prejuízos a simples opção de não se utilizar certas aplicações de redes sociais ou de mensagens. Contudo, nesta atual sociedade informacional, irá se exigir cada vez mais que todos os indivíduos se conectem não somente à internet, mas também específicos provedores de serviços *on-line*, que possuem grande poder de barganha para políticas de privacidade desfavoráveis aos usuários.

Stefano Rodotà (2008, p. 156) sintetiza que a utilização dos dados pessoais "[...] exprime a multiplicação e a intrusão de estruturas que, embora não concentrando em um único local suas possibilidades de controle [...], não tornam esse controle menos premente ou intenso".

Hoje, na sociedade cada vez mais conectada, os usuários brasileiros chegam a passar 3 horas e 39 minutos em redes sociais.[17] As ferramentas de *marketing*, dessa forma, precisaram se adaptar ao novo perfil do consumidor. Anúncios de televisão não geram o sonho de consumo como antes; por sua vez, os anúncios por meio de redes sociais são cada vez mais efetivos. Essa efetividade parte do fato de que, para usar tais redes, o indivíduo é obrigado a ser utilizado como ferramenta de personalização de anúncios.

Nunca uma máxima de marketing teve tanto sentido: "Se você não está pagando por isso, você é o produto". Não raro o mesmo anúncio de um item que se clica por acaso persegue o usuário por diferentes redes como: *Youtube*, *Facebook*, *Instagram* e outras mais. Os *cookies*, aparentemente inofensivos, armazenam e fornecem os rastros dos usuários dos sites que eles realmente visitaram (primeiras partes) às terceiras partes, que são rastreadores escondidos, tais como provedores

17 Estatísticas do relatório "2018 Global Digital" da *We Are Social* e *Hootsuite*, com base em dados de janeiro de 2018. Disponível em: <https://wearesocial.com/blog/2018/01/global-digital-report-2018> Acesso em: 15 mar. 2019.

de anúncios ligados às páginas.[18]

Com isso, não se pode mais afirmar a gratuidade para utilização das redes sociais. Em verdade, fornecem-se itens valiosos em forma de dados pessoais em troca de conteúdo de pouca relevância financeira ou intelectual para o usuário, que se vê bombardeado de publicidade direcionada por meio de perfis comportamentais. Tanto é que diversas redes sociais estão citadas como maiores companhias do mundo nos gráficos anteriores.

Não é incomum na vida cotidiana que se tenha a impressão de que os aplicativos e *sites* que o usuário acessa leiam a sua mente. Não são raros os casos em que, em uma conversa entre amigos, se comenta sobre certo produto e no próximo acesso haverá um anúncio sobre ele. Ou que uma loja que um usuário da rede social *Facebook* curtiu apareça em destaque no *site* de notícias. Ou até mesmo que se sugira ser amigos de pessoas que conheceu, mas nunca pesquisou por elas *on-line*.[19] Isto é possível graças às autorizações que são concedidas no momento do cadastro do usuário. Aplicativos que podem solicitar permissões para a escuta de áudio, que são rapidamente aceitas no *link* "Li e Aceito", por muitas vezes possuem cláusulas de rastreio por meio de *cookies* ou de tratamento da voz. Assim, algo que se comenta em voz alta pode tornar o cidadão alvo daquela publicidade específica.

Como exemplo está a assistente pessoal do *Google*, que autoriza a pesquisa por voz com a mera pronúncia da frase: "*Ok, Google*". Altamente utilizada em carros com *bluetooth* para segurança no trânsito, implica que o serviço está captando sons a todo e qualquer momento. Então, há uma vigilância intermitente, e aqueles que vigiam alegam que isso foi autorizado por cada cidadão.

18 ENGLEHARDT, Steven; NARAYANAN, Arvind. Online tracking: A 1-million-site measurement and analysis. *In*: **Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security**, October 24-28, 2016, Vienna, Áustria, doi: 10.1145/2976749.2978313. p. 02. Disponível em: <http://bit.do/fa6PJ> Acesso em: 29 nov. 2018.

19 SILVER, Curtis. How Facebook's 'People You May Know' Section Just Got Creepier. **Forbes**, 2016. Disponível em: <https://www.forbes.com/sites/curtissilver/2016/06/28/how-facebooks-people-you-may-know-section-just-got-creepier/#5d78779e5f5a> Acesso em: 15 mar. 2019.

Com isso, há o reconhecimento da importância do direito à privacidade, ao mesmo tempo há aborrecimentos quando as ações virtuais não são automatizadas. A sociedade informacional revela-se, ainda, exageradamente imediatista. Para Bruce Kasanoff (2002, p. 20): "É uma época estranha. Os defensores da privacidade estão prontos para a batalha, mas a maioria das pessoas ainda está mais aborrecida com o que as empresas esquecem sobre elas do que com o que lembram".

Imagine-se precisar realizar cadastro em todos os sites de compras em todas vezes que forem acessados, caso as empresas *on-line* não retivessem os dados. Ou até mesmo caso o lembrete de senhas do Google ou qualquer outro provedor não existisse, tendo-se que anotar em um caderno de anotações cada senha que possui, levando em conta as diferentes exigências de caracteres.

Assim, fica cada vez mais claro que os dados são o novo petróleo[20]. A principal diferenciação, contudo, resta na ausência de finitude para a coleta de dados pessoais, diferentemente da matéria fóssil. A cada dia as pessoas nascem e se transformam, sendo seus dados a verdadeira matéria-prima das conclusões que se retiram da análise dos dados pessoais.

A refinaria se dá, portanto, pelo tratamento de dados pessoais pelos gigantes de tecnologia. A partir disso, criam-se reinados invisíveis por estes gigantes, que são capazes de codificar e conhecer cada ser humano por meio de dados em seus cadastros. Ademais, ao analisar essa metáfora, poder-se-ia comparar efetivamente as grandes empresas tecnológicas a um setor que pouco demonstra preocupação com as consequências da exploração da sua matéria-prima.[21]

20 Frase atribuída a Clive Humby, em 2006, matemático que ajudou a criar o clube de fidelidade da empresa de jogos britânica Tesco, Clubcard. Em citação original: "*Data is the new oil. It's valuable, but if unrefined it cannot really be used. It has to be changed into gas, plastic, chemicals, etc to create a valuable entity that drives profitable activity; so must data be broken down, analyzed for it to have value*", recentemente reatribuída a Qi Lu, chefe de aplicações e serviços da *Microsoft*, na conferência anual para desenvolvedores, Build, em 2016.

21 CARVALHO, Victor Miguel Barros de *et al*. A Monetização de Dados Pessoais Como Alternativa a Períodos De Crise: análise jurídica a partir do marco civil da internet. In: **Congresso Internacional De Direito E Contemporaneidade:** Mídias e Direitos da Sociedade em Rede, 4, 2017, Santa Maria. Santa Maria: UFSM – Universidade Federal

As gigantes tecnológicas, alvos de diversos acrônimos,[22] sobressaíram-se no mundo em crise por partilhar um inovador modelo de negócio. Partindo de um insumo extremamente valioso, contraditoriamente barato e facilmente produzido/coletado, os serviços *on-line* se destacam dos modelos de negócios clássicos (IDEM, p. 3). É factível que a monetização de dados pessoais rende bilhões. Basta observar a receita dos maiores receptores de dados pessoais, *Google* e *Facebook*, respectivamente, $ 39,12 bilhão de dólares e $ 55,8 bilhão de dólares.[23]

Os reinados invisíveis não necessariamente incluem apenas as companhias de tecnologia, eis que mínimos aplicativos com milhares de downloads também podem gerar grandes vazamentos de dados. A internet não é um local totalmente seguro e, por vezes, está muito propícia a grandes ataques por *hackers,* os piratas modernos.

Como exemplo da vulnerabilidade dos usuários, mesmo em momento que se voluntariamente se baixa um aplicativo, está o *Brightest Flashlight Free*. Quando os celulares não possuíam a função lanterna, era necessário baixar uma aplicação para tanto. Com isso, cinquenta milhões de usuários baixaram o aplicativo *Brightest Flashlight Free*, que exigia a concordância de compartilhamento de localização. De acordo com o *Federal Trade Comission* (FTC) nos Estados Unidos, antes mesmo de se concordar, a aplicação já estava recolhendo dados e repassando a terceiras partes para direcionamento da publicidade: "Mesmo antes de um consumidor ter a chance de aceitar esses termos, o aplicativo já estava coletando e enviando informações para terceiras partes – incluindo a localização e o identificador único do dispositivo".[24]

---

de Santa Maria, 2017, p. 09. 17 p. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/9-2.pdf>. Acesso em: 15 mar. 19.

22 GAFA (*Big Four*): *Google, Apple, Facebook, Amazon*; FANG: *Facebook, Amazon, Netflix, Google*; FAAMG: *Facebook, Amazon, Apple, Microsoft e Google*.

23 Estatísticas disponíveis em: <https://www.statista.com/statistics/267606/ quarterly-revenue-of-google/> e <https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/>.

24 Tradução livre. Original: "*Even before a consumer had a chance to accept those terms, though, the application was already collecting and sending information to third parties – including location and the unique device identifier*".. ANDROID Flashlight App Developer Settles FTC

Um caso brasileiro de vazamento de dados foi o da empresa *Netshoes.* Apesar de afirmarem que não houve vazamento dos dados financeiros, os dados pessoais como nome, CPF, e-mail, data de nascimento e histórico de compras, foram acessados pelos criminosos.[25] Com o histórico de compras de um indivíduo, detém-se valiosíssima informação sobre suas variadas preferências, podendo ainda ser vendido tais cadastros a concorrentes da empresa, ação que não necessariamente vai beneficiar o usuário, que poderá ter sua conduta moldada a um perfil criado sem saber de sua existência.

Verdadeiramente, a unidade do indivíduo se dispersa, encontrando em seu lugar diversas pessoas eletrônicas, em variados bancos de dados pelo mundo, incluídas nos mais variados perfis comportamentais. A identidade da pessoa, assim, fragmenta-se em locais indeterminados e inatingíveis, de acordo com os interesses que induzem as coletas/vazamentos de informações (RODOTÀ, 2008, p. 156).

Para Fábio Konder Comparato (2008, p. 24), a transformação das pessoas em coisas se iniciou com o desenvolvimento do sistema capitalista de produção, com a denúncia de Karl Marx, transformando-se, na atualidade, na reificação do trabalhador para a do consumidor e a do eleitor.

É assim que a sociedade de vigilância se fortalece, classificando e rotulando cada um de seus indivíduos. É a sociedade que pode "[...] tornar o usuário privilegiado de um serviço, o destinatário de uma particular atenção política, o alvo de uma campanha publicitária, ou **o excluído da possibilidade de aproveitar determinadas oportunidades sociais**" (IDEM, p. 157) (grifos nossos). A "informacionalização" do ser humano é efetivamente problemática se a proteção de dados não for vista como "a cidadania do novo milênio" (RODOTÀ, 2008, p. 17).

A transmutação e ramificação do direito à privacidade passa a ser peça fundamental no estudo da proteção cibernética da humanidade, a fim de se evitar ainda mais a reificação do homem.

Charges It Deceived Consumers. **FTC website**. 2013. Disponível em: <https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-develop er-settles--ftc-charges-it-deceived> Acesso em: 15 mar. 19.

25 NETSHOES ligará para 2 milhões de clientes afetados por vazamento de dados. **Portal G1**. Disponível em: <https://g1.globo.com/df/distrito-federal/noticia/netshoes-ligara-para-2-milhoes-de-clientes-afetados-por-vazamento-de-dados.ghtml>. Acesso em: 15 mar. 2019.

2.2 A reinvenção do direito à privacidade na atualidade

A privacidade está em um constante processo evolutivo, tentando a ciência do direito acompanhar sua evolução. O direito não é um sistema de regras já postas e transmitidas, mas um conjunto de regras em movimento a serem postas e repropostas de forma contínua, consoante a doutrina de Norberto Bobbio. O objeto da ciência jurídica deve ser não tanto as regras, ou seja, as valorações dos fatos sociais que elas consistem, e sim os próprios fatos sociais de que as regras jurídicas são valorações (BOBBIO, 2007, p. 40). O direito como vetor de modificações sociais, em verdade, trata-se da assimilação jurídica das transformações sociais já ocorridas. Nesta toada, o direito à privacidade é alvo de constante "elastecimento", ao mesmo tempo em que a transformação tecnológica o faz carecer de alternativas para a sua proteção em sua perspectiva analógica.

Com isso, é relevante fazer um apanhado sobre a transformação do direito à privacidade ao que possuímos hoje.

Nas primeiras sociedades, com alguns traços remanescentes até o momento, o medo do isolamento fez os homens acreditarem que eles nunca estão integralmente sós, mesmo que se verifique a solidão física. Alan Westin, doutrinário do direito à privacidade no viés americano, afirma que em algumas sociedades as pessoas estão convencidas de que elas estão na presença ou sob observação de forças sobrenaturais, por vezes as protegendo, por vezes as ameaçando, ou simplesmente as assistindo para a ocasião do seu julgamento final.[26] Os símbolos de monitoramento da raça humana por uma entidade superior estão presentes na Bíblia, no Corão e nas representações de grandes olhos onividentes nas pinturas de mais diversas épocas (VIANNA, 2007, p. 25).

Para além de uma intrusão da privacidade humana pelas crenças no

26 Nas palavras do autor: "*The significant point is that men in most organized societies have a belief that they are watched by gods or spirits even when they are physically alone, and that personal communication with guardian spirits requires either physical or psychological privacy if it is to be most effective*". WESTIN, Alan. **Privacy and Freedom**. New York: Atheneum, 1967. p. 19. Disponível em: <https://archive.org/details/privacyfreed om00west> Acesso em: 10 abr. 2019.

sobrenatural, já se poderia vislumbrar o zelo pela vida íntima e privada a partir da desagregação da sociedade feudal para aqueles que possuíam os meios para tanto. Nas palavras de Stefano Rodotà (2008, p. 26-27):

> O isolamento era privilégio de pouquíssimos eleitos ou daqueles que, por necessidade ou opção, viviam distantes da comunidade – místicos ou monges, pastores ou bandidos. Esta possibilidade depois se estendeu a todos que dispunham dos meios materiais que lhe permitissem reproduzir, mesmo no ambiente urbano, condições que satisfaziam a esta nova necessidade de intimidade [...].
>
> A privacidade configura-se assim como uma possibilidade da classe burguesa, que consegue realizá-la sobretudo graças às transformações socioeconômicas relacionadas à Revolução Industrial. [...].
>
> **O nascimento da privacidade não se apresenta como a realização de uma exigência 'natural' de cada indivíduo, mas como a aquisição de um privilégio por parte de um grupo** (grifo nosso).

É com base na defesa da privacidade por certo grupo mais abastado que seus instrumentos jurídicos de proteção foram modelados como "característico direito burguês por excelência, a propriedade" (IDEM, p. 27). Para Danilo Doneda (2006, p. 10), o caráter iminentemente patrimonialista fez do direito à privacidade uma prerrogativa a extratos sociais determinados e, consequentemente, privilegiados.

Partindo disso, a elevação da importância da privacidade se deu, principalmente, nas sociedades ocidentais, não devendo este desenvolvimento do direito à privacidade ser aplicado às sociedades não ocidentalizadas. Como exemplo, Alan Westin, ao analisar a privacidade no mundo por ele nomeado de primitivo, a sociedade Tikopia, nas Ilhas Salomão, destacou que estes defendem os princípios de total integração social, enquanto a sociedade americana ensinaria a independência. O que pode ser visto como mínimo de privacidade para os ocidentais, por exemplo, a troca de vestimentas em ambiente recluso, em outras sociedades é inexistente tal necessidade (WESTIN, 1967, p. 11).

É importante delinear, portanto, que a visão de privacidade que se está a desenvolver é sua noção ocidental, enquanto sentida como neces-

sidade natural de cada indivíduo inserido nesta sociedade. Não se está a tentar alargar o desenvolvimento do conceito a todo o mundo.

Com essa ressalva, destaca-se que hoje as sociedades tradicionais ocidentais se direcionam, cada vez mais, para uma cultura única de massa, levando à superficialidade cultural, em que a noção de desenvolvimento econômico ideal se confunde com a ocidentalização do mundo.[27]

Partindo, assim, do histórico do direito à privacidade no ocidente, pode-se apontar como primeiro indício de manifestação legal do direito à intimidade e à vida privada as proibições da Magna Carta de 1215, em seu capítulo 39 (GUERRA, 2004, p. 34):

> Nenhum homem livre será detido ou preso, nem privado de seus bens (*disseisiatur*), banido (*utlagetur*) ou exilado ou, de algum modo, prejudicado (*destruatur*), nem agiremos ou mandaremos agir contra ele, senão mediante um juízo legal de seus pares ou segundo a lei da terra (*nisi per legale iudicium parium suorum vel per legem terre*) (COMPARATO, 2008, p. 85).

A partir dessa proteção, releva-se o Caso Semayne, de 1604, que estabeleceu o direito do senhorio em defender seu perímetro contra intrusões, prevalecendo o princípio da casa como castelo e fortaleza formulada pelo Lord Coke: "A casa de quem quer que seja é para ele o seu castelo e fortaleza, tanto para sua defesa contra a injúria e a violência, quanto para o seu repouso".[28]

Uma tentativa de formulação autônoma da privacidade, sem vinculação ao direito de propriedade, no entanto, apenas se iniciou a partir do século XIX (GUERRA, 2004, p. 34). O marco mais referenciado é repercus-

27 Nas palavras de Adam Szirmai: *"The countries that are economically and technologically advanced and politically and culturally dominant become the models for development in the eyes of their own citizens as well as in the eyes of the peoples trying to break away from their dominance. […]. This means that present-day development – which has been described above as a change in society in the direction of specific modernisation or developmental ideals – and 'Westernisation' inevitably entwined"*. (SZIRMAI, 2005, p. 11)

28 Tradução livre. Original: "*That the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose*". Court Of King's Bench. **Semayne's Case**. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html> Acesso em: 17 mar. 2019.

são nos Estados Unidos sobre o "direito de ser deixado só"[29]. Na obra *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract*, o juiz Cooley (1879) foi o primeiro a criar a expressão a ser continuamente repetida no século seguinte.

Ao criar uma classificação dos direitos, trata do "direito à imunidade pessoal" (*personal immunity*). Assim, descreve-o como: "O direito de alguém pode ser dito como o direito à completa imunidade: o direito de ser deixado só".[30] Ao continuar sua definição, contudo, em nada o relaciona à privacidade. Assim, a evolução do conceito e sua relação ao direito à privacidade apenas ocorreu com a publicação de Samuel Warren e Louis Brandeis, em 1890, pela *Harvard Law Review*: *The Right to Privacy*.

Esta obra, vista como fundamental nos estudos do direito à privacidade, trata sobre a modernidade e os males da invasão de privacidade dos recintos sagrados da vida doméstica por aparatos mecânicos de fotografia, geradores de infames notícias de jornais.[31] Os autores defenderam que o indivíduo é o único que decide sobre quais informações de sua vida privada podem ser compartilhadas.[32] Com isso, não se confundiria de forma alguma ao direito de propriedade, já que, por vezes, fotos ou cartas pessoais poderiam ser adquiridas por pessoas diversas de seus autores.[33] O que se buscaria proteger é o direito à privacidade do alvo daquele conteúdo. Nas palavras dos autores : "O objeto geral que se visa é a proteção

29 Também chamado de "o direito de ser deixado em paz". No original: "*the right to be let alone*".

30 Tradução livre. "*The right to one's person may be said to be a right of complete immunity: to be let alone*". (COOLEY, 1879, p. 29).

31 Na íntegra: "*Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able writer*". (WARREN; BRANDEIS, 1890, p. 195) .

32 Idem, p. 199.

33 Em caso célebre, *Affaire Rachel*, que envolve o direito à intimidade ocorreu na França em 1956. Nele, o Tribunal de Sena proibiu a divulgação de imagens de uma famosa atriz francesa, Elisa Rachel Félix, no leito de morte, sendo o primeiro julgado acerca do direito de imagem. (MIRANDA, 2018, p. 22).

da privacidade da vida privada".[34]

Em análise, Túlio Vianna destaca que tais autores abarcaram em um único propósito uma tríade de direitos: o de não ser monitorado, o de não ser registrado ou fotografado e o de não ser reconhecido. O mérito do argumento consistiu em proclamar a autonomia do direito à privacidade em relação ao direito à propriedade (VIANNA, 2007, p. 107). Além disso, para Laura Schertel (2014, p. 28-29), a partir dessa obra se sobressaíram as características do direito à privacidade como direito negativo, como exigência absoluta de ausência de intervenção do Estado na vida privada.

A partir desta publicação, fortifica-se no *common law* o conceito *privacy*. Leonardo Zanini propõe que o direito tratado por Warren e Brandeis é a garantia do indivíduo de "[...] uma ampla liberdade contra intromissões não desejadas em sua vida, tutelando seus pensamentos, sentimentos, emoções, dados pessoais e até mesmo o nome" (ZANINI, 2015, p. 8-27).

Contrariamente a Warren e Brandeis, Alan Westin, ao formular a sua definição de privacidade, defende que é a retirada voluntária e temporária da sociedade em geral pelo indivíduo, seja na solidão total ou na intimidade de pequenos grupos. No entanto, este desejo por privacidade não é jamais absoluto, eis que a vontade de participação do ser humano na sociedade é igualmente desejada (WESTIN, 1967, p. 7). Nisto, o autor destaca ainda características do "direito a ser deixado só". Contudo, Westin aponta também para o perigo das tecnologias que, à sua época, estavam bem mais evoluídas que as máquinas fotográficas apontadas pelos autores anteriores. O autor descrevia a preocupação social com as tecnologias de vigilância dos atos humanos, bem como as interferências oriundas desta vigilância. Em suas palavras, "Com a chegada do final da década de sessenta, era claro que a sociedade americana havia desenvolvido uma grande preocupação com a preservação da privacidade sob as novas pressões das tecnologias de monitoramento".[35]

34 Tradução livre. Original: "*The general object in view is to protect the privacy of private life*". (WARREN; BRANDEIS, 1890, p. 215)

35 Tradução livre. Original: "*As the late 1960's arrived, it was clear that American society had developed a deep concern over the preservation of privacy under the new pressures of the surveillance technology*". (WESTIN, 1967, p. 3)

Uma maior difusão do direito à privacidade nos Estados Unidos se deu com a substituição de um perfil de sociedade rural por outro perfil urbano. A eclosão desse direito relacionado diretamente ao conceito de liberdade, fortemente presente no ideário americano, foi determinante para o desenvolvimento jurídico e social daquele país (DONEDA, 2006, p. 265). Por exemplo, o *privacy* só se considerou protegido pela Constituição americana quando houve a condenação de um médico e do dono da clínica em que este trabalhava por prescrição de contraceptivos femininos, à época ilegais no estado de Connecticut. O caso, levado à Suprema Corte, gerou o reconhecimento desta lei estadual como inconstitucional, sendo destacado o respeito que merece a intimidade do casal (ZANINI, 2015, p. 24).

No Brasil, a regulação da matéria em caráter infraconstitucional se inicia pelo Código Civil de 2002, que reservou um capítulo para os direitos de personalidade, merecendo destaque o art. 21: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". O Código evidencia, ainda, no art. 11, que estes direitos são intransmissíveis e irrenunciáveis, não podendo haver limitação voluntária. O conteúdo desse artigo, no tocante à vida privada, deve ser encarado com reserva, principalmente ante a Ação Direta de Inconstitucionalidade n. 4815, que, ao questionar o art. 20 e 21 do Código Civil, mitigou o conteúdo destes artigos, destacando o balanceamento de direitos – a exemplo dos casos de biografias não autorizadas, relevando que "Biografia é história. A vida não se desenvolve apenas a partir da soleira da porta de casa".[36]

36 "[...] 2. O objeto da presente ação restringe-se à interpretação dos arts. 20 e 21 do Código Civil relativas à divulgação de escritos, à transmissão da palavra, à produção, publicação, exposição ou utilização da imagem de pessoa biografada. 3. A Constituição do Brasil proíbe qualquer censura. O exercício do direito à liberdade de expressão não pode ser cerceado pelo Estado ou por particular. 4. O direito de informação, constitucionalmente garantido, contém a liberdade de informar, de se informar e de ser informado. O primeiro refere-se à formação da opinião pública, considerado cada qual dos cidadãos que pode receber livremente dados sobre assuntos de interesse da coletividade e sobre as pessoas cujas ações, público-estatais ou público-sociais, interferem em sua esfera do acervo do direito de saber, de aprender sobre temas relacionados a suas legítimas cogitações. 5. **Biografia é história. A vida não se desenvolve apenas a partir da soleira da porta de casa**. 6. Autorização prévia para biografia constitui censura prévia particular. O recolhimento de obras é censura

Como indiscutível tendência na segunda metade do século XX, a proteção constitucional brasileira dos direitos à honra, à intimidade, à vida privada e à imagem inspirou-se na Constituição da Itália de 1947, na Lei Fundamental da República Federal da Alemanha de 1949, na Constituição Portuguesa de 1976 e na Constituição Espanhola de 1978 (FARIAS, 200, p. 128-129). As duas últimas, tratavam especificamente da intimidade, tratando a Constituição portuguesa da "reserva da intimidade privada e familiar",[37] enquanto a espanhola trata da "intimidade pessoal e familiar".[38]

Por sua vez, o reconhecimento à vida privada trata-se de um direito

judicial, a substituir a administrativa. O risco é próprio do viver. Erros corrigem-se segundo o direito, não se cortando liberdades conquistadas. A reparação de danos e o direito de resposta devem ser exercidos nos termos da lei. 7. A liberdade é constitucionalmente garantida, não se podendo anular por outra norma constitucional (inc. IV do art. 60), menos ainda por norma de hierarquia inferior (lei civil), ainda que sob o argumento de se estar a resguardar e proteger outro direito constitucionalmente assegurado, qual seja, o da inviolabilidade do direito à intimidade, à privacidade, à honra e à imagem. 8. **Para a coexistência das normas constitucionais dos incs. IV, IX e X do art. 5º, há de se acolher o balanceamento de direitos, conjugando-se o direito às liberdades com a inviolabilidade da intimidade, da privacidade, da honra e da imagem da pessoa biografada e daqueles que pretendem elaborar as biografias**. 9. Ação direta julgada procedente para dar interpretação conforme à Constituição aos arts. 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, **declarar inexigível autorização de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais**, sendo também desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas ou ausentes)". (grifos nossos). (grifos nossos) BRASIL. Supremo Tribunal Federal. **ADI 4815 DF**. Relatora: Ministra Cármen Lúcia. DJ: 01/02/2016. Disponível em: <http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADIN&s1=4815&processo=4815>, Acesso em: 18 mar. 2019.

37 "Art. 26.1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação". PORTUGAL. **Constituição da República Portuguesa**. Disponível em: <https://www.parlamento.pt/Legislacao/paginas/constitu icaorepubli caportuguesa.aspx> Acesso em: 3 jun. 2019.

38 Art. 18.1. "É garantido o direito à honra, à intimidade pessoal e familiar e à própria imagem". ESPANHA. **Constituição Espanhola**. Disponível em: <https://www.tribunalconstitucional.es/es/tribunal/normativa /Normativa/CEportugu%C3%A9s.pdf> Acesso em: 3 jun. 2019.

fundamental, garantido pela Constituição brasileira no art. 5º, inciso X, [39] com consequentes deveres negativos e, principalmente, deveres positivos por parte do Estado. A privacidade, aspecto mais amplo que a intimidade, é um conjunto das facetas da vida de uma pessoa, possibilitando que se tenha um retrato de sua vida íntima e sua personalidade pessoal, familiar e social (VIEIRA, 2001, p. 72). Esses direitos, previstos tanto no Código Civil como na Constituição Federal, constituem rol exemplificativo, já que a sua visão como cláusula geral aberta não os deixa estanques e paralisados no tempo (BLUM, 2018, p. 35).

Na Constituição Federal, portanto, o direito à privacidade possui tanto a feição de direito da personalidade como o de direito fundamental. Com isso, esses direitos possuiriam duplo caráter, além de constituírem direitos fundamentais com sua proteção inerente, são ao mesmo tempo direitos da personalidade. Os direitos de personalidade, incluído neles o direito à privacidade, nascem do próprio homem, sendo ligados diretamente à projeção da pessoa na sociedade, e dotam-se de características que limitam a ação do titular, como a intransmissibilidade, a imprescritibilidade, a irrenunciabilidade e a inexpropriabilidade (GUERRA, 2004, p. 34-38). Esses direitos,[40] previstos tanto no Código Civil quanto na Constituição Federal, constituem rol exemplificativo, já que a sua visão como cláusula geral aberta não deixa tais direitos estanques e paralisados no tempo (IDEM, 2018, p. 35).

Para Danilo Doneda (2006, p. 28), uma proteção integrada e dirigida pela tábua axiológica constitucional seria uma boa estratégia para a tutela integral da personalidade. Contudo, a tradição jurídica brasileira privilegiou a proteção com focos de atuação determinados, a exemplo das previsões do Código de Defesa do Consumidor, prevalecendo a lógica do seu campo específico. Esse tratamento esparso brasileiro da vida privada como direito da personalidade passou a ser transformado a partir da pro-

39 Art. 5ª, X: São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

40 Para Adriano de Cupis (2008, p. 21): "A personalidade, se não se identifica com os direitos e com as obrigações jurídicas, constitui a precondição deles, ou seja, o seu fundamento e pressuposto".

mulgação da Lei Geral de Dados Pessoais.

O seccionamento entre a vida privada e a intimidade, apesar de ambas alcançadas pelos direitos de personalidade, ainda gera discussões sobre suas próprias particularidades. A exemplo da doutrina americana, o *privacy* não se confunde com a intimidade. Para Robert S. Gerstein (1978, p. 76-81), a intimidade não existiria se as pessoas não tivessem a oportunidade de exercerem a privacidade. A intimidade, neste conceito, está centrada na exclusão de outros e na possibilidade de se ressentir de suas intrusões desmedidas.

Assim, o direito à privacidade e à intimidade, apesar de possuírem pontos de convergência, não se confundem, mas em verdade se completam. Partindo da doutrina alemã, que surgiu principalmente a partir do caso Elfes[41], distingue-se três esferas, com intensidades de proteção decrescente:

> [...] a *esfera mais interior* ("último e inviolável âmbito de liberdade humana", "âmbito mais interno (íntimo)", "esfera íntima inviolável", "esfera nuclear da configuração da vida privada, protegida de forma absoluta"), a *esfera privada ampliada*, que inclui o âmbito privado que não pertence à esfera mais interior, e a *esfera social*, que inclui tudo aquilo que não for atribuído nem ao menos à esfera privada ampliada (grifos do autor) (ALEXY, 2014, p. 341).

Assim, o direito à privacidade teria surgido de um "elastecimento" do direito à intimidade, possuindo em ambos maior ou menor restrição do grau da informação pessoal (VIEIRA, 2001, p. 70). A esfera privada, em sentido estrito, comunica o indivíduo com a sociedade; a esfera intermediária trata da intimidade e as informações mais restritas do ser humano; e a esfera do segredo contém as escolhas subjetivas do indivíduo, que fogem ao interesse público (MIRANDA, 2018, p. 26-27).

No entendimento de Sidney Guerra (2004, p. 55), a intimidade iria além da vida privada, por se caracterizar como impenetrável, intransponí-

41 *BVerfGE* 6,32. Houve interpretação pelo Tribunal Constitucional Federal Alemão que o direito ao livre desenvolvimento da personalidade é um direito à liberdade geral de ação. (ALEXY, 2014. p. 341).

vel, dizendo respeito unicamente ao seu titular, enquanto a vida privada seria peculiar à família, à saúde física e mental e aos hábitos sexuais, sendo possível seu compartilhamento com familiares e amigos próximos. Já para Sérgio Carlos Covello (1999, p. 7), os termos "privacidade" e "intimidade" devem ser tratados como sinônimos, já que a palavra privacidade, de tradução errônea do termo *privacy*, não é de boa cepa vernácula. O vernáculo intimidade, por sua vez, é preferível por ser mais expressivo entre juristas de língua espanhola, contendo bem a ideia do *privacy*, podendo-se dizer que o direito à intimidade é expressão equivalente ao *right to privacy*. No mesmo sentido, o filólogo Napoleão Mendes de Almeida, ao defender o termo privatividade:

> **Privatividade** – Essa é a palavra portuguesa, não 'privacidade'. [...] O adjetivo é *privativo,* e dele temos *privatividade,* para indicar 'qualidade de *privativo*'. Não pensemos em *privação,* nem nos deixemos levar por *vivacidade*, que também provém de adjetivo (*vivaz*) e tem o justificado por corresponder à gutural do radical latino (*vicac*-is) (grifos do autor). (ALMEIDA, 1981, p. 246)

Apesar da discussão, não menos importante, sobre eventual tentativa de tradução direta em termo e conteúdo do *privacy* para o português, em momento algum o constituinte se utiliza do termo privacidade. Seu objetivo foi enumerar, de forma seguida, os vocábulos intimidade e vida privada. Os termos são, por vezes, vistos como sinônimos, contudo acredita-se possuírem alcances diferentes, tanto que ambos foram tratados de forma consecutiva na mesma frase, não se tratando de mera redundância.

Enquanto a vida privada, à semelhança da figura do *Lord Coke* como princípio da casa como castelo e fortaleza, diz respeito à privacidade nas suas relações interpessoais, a intimidade diz respeito a um núcleo mais profundo do indivíduo em conexão consigo mesmo, sobre o conhecimento de seus limites, seus desejos e seus objetivos de vida.

Com isso, após a análise histórica da transformação e consequente reinvenção do direito à privacidade, percebe-se, hoje, que o custo da proteção da privacidade é visto como muito elevado, já que sua valorização só é significativa quando ele é zero. Para oportunidade de se receber um

desconto em troca da abertura da sua vida privada, existem milhares de voluntários prontos à disponibilização dos dados (KASANOFF, 2002, p. 20). Ao analisar o art. 17[42] do Pacto Internacional sobre Direitos Civis e Políticos, ratificado pelo Brasil em 1992, Fábio Konder Comparato (2008, p. 313) assinala: "É lamentável, pois, reconhecer que o direito à privacidade tende a transformar-se, na atual era da informática, em piedosa ficção [...]".

Por sua vez, o surgimento das redes sociais mistifica o debate sobre o limite entre o público e o privado na vida de cada um (BRANCO, 2017, p. 47). Para Sérgio Branco, "trata-se da mais nova releitura da constatação de Philippe Artières de que o anormal é o sem-papéis. O anormal, agora, é o *sem-perfil*" (IDEM, p. 48). Ainda, para Gilberto Dupas (2001, p. 17): "O homem volta a ser rei exibindo a sua intimidade com os objetos de consumo ou identificando-se com os novos ícones, os heróis da mídia eletrônica transformados eles mesmos em mercadoria ou identificados com marcas globais".

O excesso de imagens a que o homem se submete submetemos e o apego à imagem instantânea, descartada em vinte e quatro horas, revela contornos sociais jamais vistos. Os registros na internet se transformaram na maneira em que cada pessoa se tornou a sua "própria arquivista" (BRANCO, 2017, p. 59). O estrangeirismo *stalker*, que pode ser traduzido como perseguidor, já foi transformado em gíria verbal, com uma conotação menos severa: "stalkear",[43] com sentido de se informar sobre a vida alheia. Isto se torna cada vez mais interessante ao mesmo tempo em que se precisa de uma aprovação externa em todas as publicações em redes.

A curiosidade, não sendo característica presente apenas nos seres humanos, mas também em outros animais, é ilustrada nos mitos das mais

42 ARTIGO 17 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

43 "Stalkear, verbo transitivo: quem stalkeia, stalkeia alguém. Sempre. Stalkear, verbo intransitivo: o stalker eventualmente se perde, se acha e se basta no próprio stalkeamento. Já não faz muita diferença a quem espiona, que vidas acompanha, com que motivação. Um dia, sem nem perceber, terá feito da perseguição um fim em si mesma – uma perseguição, portanto, sem fim". ESSENFELDER, Renato. Stalkear, verbo intransitivo. **Estadão**. Disponível em: <https://emais.estadao.com.br/blogs/renato-essenfelder/stalkear-verbo-intransitivo/> Acesso em: 17 mar. 2019.

variadas sociedades, com grandes consequências para aqueles que não conseguem controlá-la. Entre eles estão a caixa de Pandora, a mordida da maçã por Eva, a morte de Orfeu por Hades, Eros e Psiquê. Alan Westin estabelece a curiosidade como um dos elementos da privacidade. Para o autor, são ilusórios os ditames que cada um cuida da sua vida, já que existe o desejo inerente aos membros da sociedade de penetrar os segredos alheios. Enquanto a curiosidade é pertencente à invasão de um indivíduo pelo outro, a vigilância se dá quando a invasão ocorre pelas autoridades. Essa vigilância é necessária em alguns aspectos, principalmente para a eficácia das normas sociais (WESTIN, 1967, p. 20).

Enquanto o direito ao respeito da vida privada reflete um componente eminentemente individualista, a proteção de dados é uma proteção dinâmica, segue seus rastros em todos os momentos. Assim, de acordo com Rodotà:

> É de fato o fim da linha de um longo processo evolutivo experimentado pelo conceito de privacidade – de uma definição original como o direito de ser deixado em paz, até o **direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída**. [...]. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio (grifo nosso) (RODOTÀ, 2008, p. 17).

Este direito de controle sobre as informações, contudo, até certo ponto, poder-se-ia ser considerado utópico. Os dados pessoais, que depois se transformam em informações, disseminam-se não apenas em velocidade inimaginável na rede, mas para locais que não se pode rastrear completamente. O direito de não ser registrado, como vertente do direito à privacidade, é garantia contra as violações do direito à igualdade (VIANNA, 2007, p. 115). Relembrando experiências passadas da humanidade, aduz Túlio Vianna:

> A experiência nazista demonstrou que para discriminar é necessário antes de tudo registrar a população traçando um mapa das características de cada indivíduo. Estes registros são os instrumentos de filtragem da população, pelos quais o poder seleciona e exclui os indivíduos julgados indesejáveis (IDEM, p. 115).

Com isso, pode-se dizer que o direito à privacidade abre mais um de seus leques, para fortalecer o direito à proteção de dados pessoais. "A proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea" (RODOTÀ, 2008, p. 21).

Danilo Doneda (2006, p. 30) destaca que, partindo da proteção de dados pessoais, [a proteção da privacidade] deixa de dar vazão somente a um imperativo de ordem individualista, mas passa a ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que na disciplina da privacidade passe a se definir todo um estatuto que acaba por compreender as relações da própria personalidade com o mundo exterior.

É necessário o alargamento da perspectiva institucional, superando a lógica unicamente da propriedade, diferenciando a disciplina de acordo com as funções para as quais são destinadas as informações coletadas, analisando com profundidade os interesses envolvidos para colocar em funcionamento novos critérios de equilíbrio de tais interesses (RODOTÀ, 2008, p. 50).

O direito à privacidade foi inicialmente instituído na premissa clássica "pessoa-informação-sigilo", que se transmuta em "pessoa-informação--circulação-controle", assim, Rodotà articula a ulterior definição do direito à privacidade como "o direito de manter o controle sobre as próprias informações e de *determinar as modalidades de construção da própria esfera privada*" (IDEM, p. 93-109). [grifos do autor]

No entanto, o conceito de evolução do direito à privacidade, de acordo com João Carlos Zanon, deve ser visto com reservas, pois o vocábulo evolução traria uma carga semântica de melhoria e progresso, acarretando uma falsa impressão. O que haveria, em verdade, é uma ampliação do conceito (ZANON, 2013, p.67). Apesar de tais considerações, acredita-se na evolução do conceito consoante a evolução da sociedade para uma sociedade de informação. A evolução, neste sentido de transformação, não necessariamente implica em melhorias, mas sim em mudanças a partir da construção de novas necessidades.

A difusão de informações sem o compromisso com a veracidade é um dos verdadeiros dilemas do século XXI: a tentativa de contenção do

conteúdo produzido na internet. Além do dilema, o maior obstáculo hoje é lidar com essa nova privacidade na transformação do tempo e espaço da sociedade digital. Com o tempo de difusão da informação reduzido a milésimos de segundos a distâncias antes inconcebíveis, revela como nova característica do direito à privacidade a relevância ao controle desta exercido pelo próprio indivíduo.

Em algum momento de seu processo evolutivo, o direito à privacidade pode ter se bastado na perspectiva individualista. No entanto, a partir do momento que dados de sua vida privada gera lucro a terceiros, a perspectiva individualista não se basta, sendo necessário a inclusão de novos interesses para que o balanço constitucional esteja correto e a fundamentalidade da intimidade e da vida privada estejam efetivamente protegidas.

2.3 O informacionalismo e o panóptico como construção do direito à autodeterminação informativa

O direito à privacidade está na constante tensão entre a desvinculação do direito à propriedade, ao mesmo tempo em que se defende o controle integral das próprias informações. No entanto, seria possível o controle da forma em que o indivíduo é visto na sociedade?

Manter-se informado sempre foi privilégio de poucos. No início das formações sociais, em que a grande maioria da população era analfabeta, os escritos se produziam em velocidade lenta e, em sua maioria, eram censurados por alguma autoridade. A informação era transmitida boca a boca, sem grande força para a disseminação. A dificuldade de arquivamento da informação também era um obstáculo, tarefa confiada a poucos, que não necessariamente estariam comprometidos com a realidade.

A situação está radicalmente alterada hoje, tendo como principal motivo a facilidade de arquivamento da informação. Para entender o princípio da autodeterminação informativa é preciso, primeiro, entender o conceito da sociedade de informação. Manuel Castells (2008, p. 43), ao traçar a transformação histórica da sociedade, denota que a revolução da tecnologia da informação teve como importante base o caráter libertário dos movimentos dos anos 1960 nos Estados Unidos – partindo da cultura de li-

berdade, as tecnologias de informação foram mais facilmente difundidas.

Segundo o autor, a origem da internet se deu para impedir uma eventual tomada ou destruição do sistema norte-americano de comunicações pelos soviéticos, em caso de guerra nuclear (IDEM, p. 44). Com isso, criou-se uma arquitetura em rede – ARPANET – que não pode ser controlada de nenhum centro e é composta por inúmeras maneiras de conexão, contornando a existência de barreiras eletrônicas (IDEM, p. 44). Em tempos de guerra, mesmo que fria, garantir a privacidade das informações governamentais é sinônimo de garantia da segurança.

Em meio a este turbilhão de novos acessos às tecnologias informacionais, iniciou-se uma noção, mesmo que incipiente, da importância dos dados nos novos tempos e, mais precisamente, da importância da conversão dos dados em informação, devidamente tratada e estratificada.

Vale destacar a divisão entre os modos de produção e modos de desenvolvimento. Os modos de produção, que pode ser capitalista ou estatista, são regidos "pelas relações de classes no processo produtivo", enquanto os modos de desenvolvimento agrário, industrial ou informacional, são os "procedimentos mediante os quais os trabalhadores atuam sobre a matéria para gerar um produto". Com isso, Castells (2008, p. 51-53) defende o novo modo de desenvolvimento social, o "informacionalismo", surgido da necessária reestruturação do capitalismo no final do século XX.

> No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos. [...] Como o informacionalismo baseia-se na tecnologia de conhecimentos e informação, há uma íntima ligação entre cultura e forças produtivas e entre espírito e matéria, no modo de desenvolvimento informacional. Portanto, devemos esperar o surgimento de novas formas histórias de interação, controle e transformação social (IDEM, p. 53-54).

Tendo em vista que sua teorização ocorreu no final da década de 1990, seu prospecto estava correto, principalmente quanto ao surgimento de novas formas de controle social. A vigilância intermitente de empresas e do Estado tornou-se uma realidade, o que destaca a obra do utilitaris-

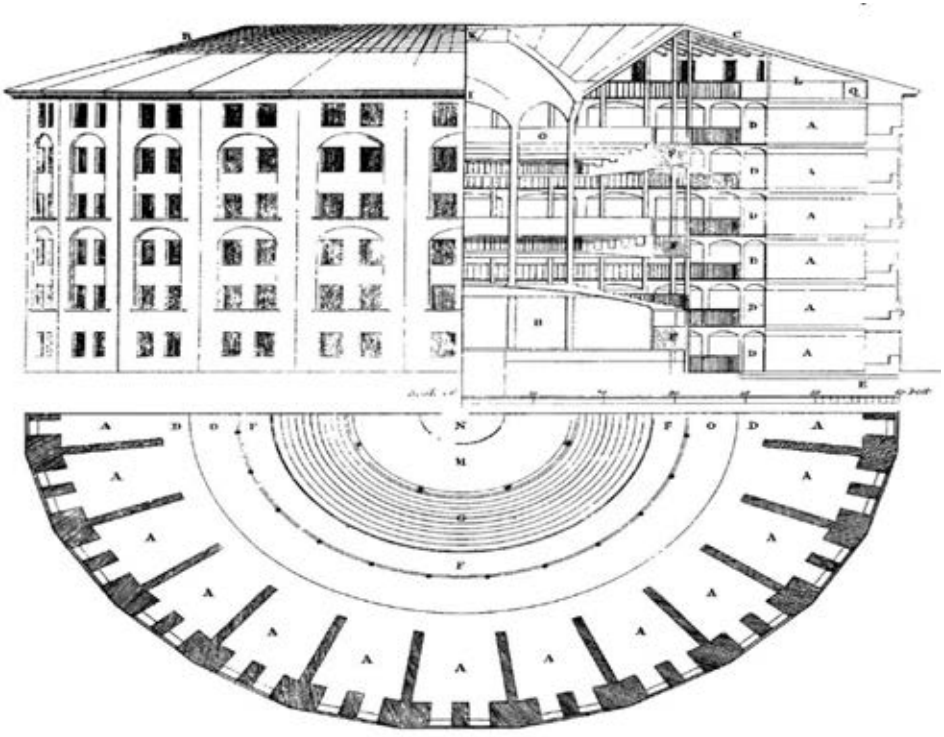
ta Jeremy Bentham sobre o Panóptico (ou Casa de Inspeção). Sua obra consiste em uma coletânea de cartas escritas em 1787, enquanto o autor estava na Rússia, endereçadas a um amigo na Inglaterra. Nelas, consigna a ideia de um novo princípio de construção aplicável a quaisquer tipos de pessoas que precisem ser mantidas sob inspeção.[44]

Descreve a sua criação de uma prisão circular, ou qualquer edifício feito para o monitoramento, [45] com uma torre central chamada de alojamento do inspetor. Esta torre, que conteria o observador, seria repleta de persianas que possibilitavam a observação completa dos prisioneiros, sem que, por sua vez, estes conseguissem algum vislumbre de quem os observava.

44 Título e descrição pelo próprio autor, no início de seu ensaio (BENTHAM, 2008, p. 15).

45 Em continuação de seu pensamento, Jeremy Bentham afirma: "Para dizer tudo em uma palavra, ver-se-á que ele é aplicável, penso eu, sem exceção, a todos e quaisquer estabelecimentos, nos quais, num espaço não demasiadamente grande para que possa ser controlado ou dirigido a partir de edifícios, queira-se manter sob inspeção um certo número de pessoas. Não importa quão diferentes, ou até mesmo quão opostos, sejam os propósitos: seja o de punir o incorrigível, encerrar o insano, reformar o viciado, confinar o suspeito, empregar o desocupado, manter o desassistido, curar o doente, instruir os que estejam dispostos em qualquer ramo da indústria, ou treinar a raça em ascensão no caminho da educação, em uma palavra, seja ele aplicado aos propósitos das prisões perpétuas na câmara da morte, ou prisões de confinamento antes do julgamento, ou casas penitenciárias, ou casas de correção, ou casas de trabalho, ou manufaturas, ou hospícios, ou hospitais, ou escolas" (BENTHAM, 2008. p. 19-20).

FIGURA 3 – PLANO DO PANÓPTICO[46]



Fonte: REVELEY, Willey. **The Works of Jeremy Bentham**, 1791. Disponível em: <https://commons.wikimedia.org/wiki/File:Panopticon.jpg> Acesso em: 12 jun. 2019.

Essa estrutura em que de um lado há aquele que tudo sabe e que tudo vigia, enquanto do outro lado expõe-se os vigiados que permanecem na ignorância, passa a ser uma metáfora para a exploração de dados na atualidade. Na figura a seguir, há claro exemplo com a empresa Facebook, mas poderia ser facilmente substituída por quaisquer empresas que possuam como modelo de negócio a exploração de dados pessoais.

46 Tradução livre: "*Plan of the Panopticon*".

FIGURA 4 – FACEBOOK: O PANÓPTICO DA IDADE MODERNA[47]

Fonte: Autor desconhecido. Disponível em: <http://tiny.cc/a0167y> Acesso em: 12 jun. 2019.

Michel Foucault, em sua crítica à criação de Bentham e antes de descrever a sociedade disciplinar, assim descreve o panóptico:

> [O panóptico] é o diagrama de um mecanismo de poder levado à sua forma ideal: seu funcionamento, abstraindo-se de qualquer obstáculo, resistência ou desgaste, pode ser bem representado como um puro sistema arquitetural e óptico: é na realidade uma figura de tecnologia política que se pode e se deve destacar de qualquer uso específico (FOUCAULT, 2014, p. 199).

O panóptico, portanto, passou a ser termo e modelo crucial ao estudo da sociedade informacional e de suas consequências, entre elas, a constante vigilância estatal e empresarial.

47 Tradução livre. "Facebook: *The Panopticon of Modern Age*". Autor desconhecido. Disponível em: <http://tiny.cc/a0167y> Acesso em: 12 jun. 2019.

Para Byung-Chul Han (2018), no panóptico digital não é possível que haja qualquer manifestação de confiança. "A confiança torna possível relações com outros sem conhecimentos precisos sobre eles. A possibilidade de uma aquisição rápida e fácil de conhecimento é prejudicial à confiança". Essa falta de confiança daria lugar ao controle, de forma que a sociedade de transparência seria, em verdade, uma sociedade de vigilância. Assim, em vez de um isolamento prisional, na atual sociedade se teria uma hipercomunicação que facilita o controle total por quem quer que possua os meios (HAN, 2018).

A sociedade em geral tornou-se mais ciente do risco da utilização de seus dados a partir das revelações de Edward Snowden, em 2013, [48] sobre as informações dos programas de segurança Agência Nacional de Segurança dos Estados Unidos (NSA), revelando a captação de comunicações de milhares de pessoas no mundo.[49]

Ainda, de forma mais recente, a importância da informação no mundo moderno se destaca com o escândalo ligado à consultoria *Cambridge Analytica*. Tal empresa se utilizou de dados do *Facebook* em campanhas eleitorais para "microdirecionamentos" de publicidade eleitoral, havendo um despertar geral para a importância da proteção de dados na internet.

As informações foram obtidas por um acadêmico do Reino Unido por meio de um teste on-line utilizado por milhares pessoas que exigia o cadastro por meio do Facebook. Assim, por haver uma possibilidade de exploração nos "Termos de Uso do *Facebook*", permitiu-se que cada usuário

48 Cf. HODGSON, Sam. Edward Snowden: 'Do I Think Things Are Fixed? No.' **The New York Times**. Disponível em: <https://www.nytimes.com/2016/12/07/opinion/edward-snowden-do-i-think-things-are-fixed-no.html> Acesso em: 4 jun. 2019.

49 Han (2018) continua: "Os habitantes do panóptico digital não são prisioneiros. Eles vivem na ilusão da liberdade. Eles abastecem o panóptico digital com informações que eles emitem e expõem voluntariamente. A autoexposição é mais eficiente do que a exposição por meio de outro. Aí reside um paralelo com a autoexploração. A autoexploração é mais eficiente do que a exploração por outro porque ela é acompanhada do sentimento de liberdade. Na autoexposição a exibição pornográfica e o controle panóptico coincidem. A sociedade de controle tem a sua consumação lá, onde os habitantes se comunicam não por coação exterior, mas sim por carência interna, onde, então, o medo de ter de abdicar de sua esfera privada e intima dá lugar à carência de se colocar desavergonhadamente à vista, ou seja, onde a liberdade e o controle são indistinguíveis".

consentisse a exploração de dados de seus amigos, sem o conhecimento destes. Ao todo, com o efeito de rede, foram 87 milhões de pessoas com seus perfis explorados, entre elas o do próprio Mark Zuckerberg, o fundador e CEO do Facebook.[50]

O modelo panóptico de Jeremy Bentham, portanto, ganha força na consciência social da pós-modernidade. No meio dos símbolos, por sua vez, já se aborda de forma reiterada a revolução das máquinas e a mecanização do homem como o sinal de novos tempos. Manifestações culturais e de entretenimento, como as figuras *Skynet* e *Matrix*, são parte do inconsciente de uma geração. Sobre a *Matrix*, na análise de Túlio Vianna: "*Matrix* é a manifestação simbólica da luta do homem para impedir que a tecnologia que é ferramenta se torne arma de dominação do homem pelo homem" (VIANNA, 2007, p. 51).

A tecnologia que tanto facilita a vida hodierna apresenta limitações quanto ao resguardo de certos direitos dos seres humanos. Por meio dela se está a permitir abusos econômicos de maior importância, não havendo, no presente momento, ferramentas de proteção pelo usuário comum que estejam à altura das ferramentas utilizadas para monitoramento e intrusão em suas vidas.

Os dados do indivíduo em uma sociedade de informação são um bem imaterial de valor econômico que cresce em progressão geométrica, em tempos que a informação alimenta e gera mais informação de forma pouco controlável.

Assim, o direito à informação[51] ganhou grande importância nos últimos tempos em todo o mundo, mas não deve ser encarado como irrestrito, eis que abrange um leque, tal como o "direito de informar, o de se informar e o de ser informado" (BOFF et al., 2018, p. 9).

Uma suposta tensão entre o direito à privacidade e o direito à informação transforma o próprio direito à privacidade, sendo necessária a

50 BADSHAH, Nadeem. Facebook to contact 87 million users affected by data breach. *The Guardian*, 2018. Disponível em: <https://www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach> Acesso em: 25 abr. 2019.

51 No Brasil, o direito à informação é reconhecido pela Constituição Federal no artigo 5º, incisos XIV e XXXIII, reconhecendo-se este como direito fundamental para a vida em sociedade.

reflexão sobre a fronteira entre a vida privada e a necessidade de se manter informado na vida cotidiana. A partir de ambos, em que não há uma relação de superioridade, transmuta-se no contexto tecnológico o direito à autodeterminação informativa.

Para a construção desse direito, é necessário destacar que ele se desenvolve a partir do direito à informação. A evolução para uma sociedade informacional foi gradativa, sofrendo eventuais retardamentos durante as grandes guerras. De forma a recuperar o retrocesso, em 1948, a Declaração Universal dos Direitos Humanos, [52] destaca em seu artigo XIX: "Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e idéias por quaisquer meios e independentemente de fronteiras." [53]

Apesar da inegável importância da Declaração Universal dos Direitos Humanos, uma maior disseminação (VIEIRA, 2001, p. 79) do direito à informação se deu com a Igreja Católica, com a Encíclica *Pacem in Terris* do Papa João XXIII, de 1963:

> Direitos que se referem aos valores morais e culturais
> 12. Todo o ser humano tem direito natural ao respeito de sua dignidade e à boa fama; direito à liberdade na pesquisa da verdade e, dentro dos limites da ordem moral e do bem comum, à liberdade na manifestação e difusão do pensamento, bem como no cultivo da arte. Tem direito também à informação verídica sobre os acontecimentos públicos. [...]
> [...]
> 90. Exige ainda a verdade que nas múltiplas iniciativas, através da utilização das modernas invenções técnicas, tendentes a favorecer um maior conhecimento recíproco entre os povos,

52 Quanto ao direito à privacidade e intimidade, a Declaração Universal dos Direitos Humanos, em seu artigo XII, dispõe: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques". ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Declaração Universal dos Direitos Humanos**. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 19 mar. 19.

53 Idem, ibidem.

> se adotem rigorosamente critérios de serena objetividade. Isto não exclui ser legítima nos povos a preferência a dar a conhecer os lados positivos da sua vida. Devem, porém, ser totalmente repudiados os métodos de informação que, violando a justiça e a verdade, firam o bom nome de algum povo.[54]

Esta encíclica, para além do conteúdo religioso, divulga a milhares de fiéis sobre a necessidade de "informação verídica sobre os acontecimentos públicos", bem como que devem "ser totalmente repudiados os métodos de informação que, violando a justiça e a verdade, firam o bom nome de algum povo". Além da capacidade de divulgação, revela conteúdo muito alinhado com a atualidade, principalmente se se considerar o impacto crescente das notícias falsas no mundo.

No Brasil, o direito à informação está previsto em diversos incisos do art. 5º da Constituição Federal, inicialmente pelo inciso XIV: "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional", passando ao inciso XXXIII: "todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado" e inciso LXXII: "conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público".

Na doutrina brasileira, Paulo Bonavides (2015, p. 585) considera o direito à informação como direito fundamental da quarta geração – para ele, corresponde à última fase do Estado Social e é o coroamento da globalização política:

> São direitos da quarta geração o direito à democracia, o direito à informação e o direito ao pluralismo. Deles depende a concretização da sociedade aberta do futuro, em sua dimensão de máxima universalidade, para a qual parece o mundo inclinar-se no plano de todas as relações de convivência. (IDEM, p. 586)

54 PAPA JOÃO XXIII. **Carta Encíclica *Pacem In Terris***. Disponível em: <http://w2.vatican.va/content/john-xxiii/pt/encyclicals/documents/hf_j-xxiii_enc_11041963_pacem.html#_ftn45>. Acesso em: 19 mar. 2019.

Necessário citar, ainda, a Lei de Acesso à Informação [55] Lei n. 12.527/2011, que destaca o direito constitucional de acesso às informações públicas, regulamentando o art. 5º, inciso XXXIII, art. 37, §3º, inciso II e art. 216, §2º da Constituição Federal. Tal norma insere verdadeiramente o país num contexto mundial de respeito ao direito do cidadão em manter-se informado (BOFF, 2018, p. 51). Na legislação, há seção própria sobre o tratamento de informações pessoais, inserindo em seu art. 31 disposição sobre o tratamento de dados pessoais, destacando que este deve se dar de "forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais".[56]

Neste breve histórico, precisa-se destacar o caso mais sensível em que o processamento automático de dados mostrou seu potencial seletivo e excludente. A identificação de judeus na Alemanha nazista se deu com o uso de cartões perfurados, tecnologia criada pela *International Business Machines*

55 A criação de leis de acesso à informação, principalmente na América do Sul, trata-se da consolidação do Estado Democrático de Direito, conferindo aos cidadãos condições para a participação política. (MIRANDA, 2018. p. 251-252)

56 Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I – terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: I – à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico; II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem; III – ao cumprimento de ordem judicial; IV – à defesa de direitos humanos; ou V – à proteção do interesse público e geral preponderante. § 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

(IBM), que automatizava o tratamento da informação. Assim, o recenseamento alemão identificou com precisão os judeus na população, partindo desses dados a lei para "Prevenção da Prole com Doença Genética", evoluindo, ao final, a uma pseudociência de raça. A técnica dos registros por meio de cartão perfurado demonstra que o poder da informação permitiu um dos maiores massacres da história (VIANNA, 2007, p. 95-102). Este histórico demonstra, para Túlio Vianna, "a potencialidade seletiva e excludente dos bancos de dados informatizados e recomenda estudos jurídicos no sentido de limitar a coleta e o armazenamento de informações pessoais seja pelo Estado ou por instituições privadas" (IDEM, p. 103).

Não é de se espantar, com isso, que a rubrica do direito à autodeterminação informativa tenha surgido na Corte Constitucional Alemã. Foi produzido o chamado acórdão de 25 de março de 1982 sobre o Censo (*Volkszählungsurteil)*, que analisou a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho". O caso se delineia pois, neste mesmo ano, foi decretada a realização de um censo geral da população, tendo, como parte declarada, o objetivo de obter as características sociais e demográficas da população, bem como o status econômico desta. Contudo, entre as provisões deste ato censitário estava a possibilidade de cruzamento das informações entre as autoridades federais e municipais de forma anônima para verificar a veracidade das informações fornecidas (MENDES, 2014, p. 31). Além disso, outros pontos suscitaram controvérsia, como a previsão de multa a quem não quisesse responder ao Censo, bem como a inserção de mecanismos que favorecessem a denúncia destas pessoas (DONEDA, 2006, p. 193).

Com isso, a Corte, considerando as modernas condições de tratamento, de arquivamento, de uso e de transferência de dados, julgou pela constitucionalidade da Lei em geral, declarando os dispositivos que determinavam a comparação de dados e transferência entre órgãos nulos (MENDES, 2014, p. 31), de forma a resguardar a proteção do indivíduo a partir dos direitos da personalidade, com base no artigo 2.1 combinado com o artigo 1.1 da Lei Fundamental Alemã.[57]

57 Lei Fundamental da República Federal da Alemanha. Artigo 1 [Dignidade da pessoa humana – Direitos humanos – Vinculação jurídica dos direitos fundamentais] (1) A

Com isso, as restrições ao chamado direito à autodeterminação informativa (*rechts auf informationelle Selbstbestimmung*) só seriam permitidas em caso de manifesto interesse público, com comprovada base legal e constitucional.[58]

Quanto à fundamentalidade deste direito, Ana Sanden (2014, p. 89-90) defende que não houve a criação de um novo direito fundamental, e sim a proteção dos direitos de personalidade contra os riscos dos novos avanços tecnológicos, já que o direito à autodeterminação informativa, apesar de aparentemente criado no acórdão, já possuía fundamentos na legislação alemã.[59] A autora desenvolve que este direito é uma fórmula jurídica capaz de encarnar dilemas do processamento automático da informação, sendo a solução encontrada mais adequada ao dilema.

Na mesma linha, Stefano Rodotá (2008, p. 45) afirma que, ampliando o princípio de consentimento, o Tribunal Constitucional Alemão afirma um direito à autodeterminação informativa com valor constitucional.

Laura Schertel, em sentido contrário, defende que houve a criação de um direito subjetivo fundamental que deve ser observado e concretizado pelo legislador, não podendo, por isso, ter seu núcleo fundamental violado. "Isso significa uma limitação ao poder legislativo, que passa a estar vinculado à configuração de um direito à autodeterminação da informação" (SCHERTEL, 2014, p. 31). O direito à informação surge, então, de um contexto político de luta por direitos. No mesmo sentido se posiciona Danilo Doneda.[60]

---

dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público. Artigo 2 [Direitos de liberdade] (1) Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral. ALEMANHA. **Lei Fundamental da República Federal da Alemanha**. Disponível em: <https://www.btg-bestellservice.de/pdf/80208000.pdf> Acesso em: 19 mar. 19

58 BVerfG, *Volkszählungsurteil*, 15.12.83. Acórdão traduzido para o inglês. Disponível em: <https://freiheitsfoo.de/census-act/> Acesso em: 19 mar. 19

59 A autora continua: "Com efeito, ela atende, de um lado, à necessidade de fortalecer a posição do indivíduo, atribuindo-lhe o direito de ter controle sobre as informações relativas a ele. Por outro lado, ela não fecha as portas ao processamento automático da informação relativa à pessoa, permitindo, sob determinadas condições, que medre a liberdade de informação" (SANDEN, 2014, p. 89-90).

60 "Concebido como um direito fundamental, na esteira do direito geral de personali-

Este último defende, ainda, que a ideia da autodeterminação informativa não foi inovação da corte alemã, eis que já estava presente na doutrina de Alan Westin. Contudo, o autor americano não defendeu a autodeterminação informativa como ideia autônoma, apenas incluindo-a para delimitar a sua definição de privacidade, que já era deveras atualizada para o tempo que fora criada: "Privacidade é a reivindicação de indivíduos, grupos, ou instituições para determinar para si mesmos quando, como e até que ponto a informação sobre eles é comunicada a outrem".[61]

Contudo, ao fazer a defesa cega deste instituto, criado para um país muito diferente do Brasil, poder-se-ia incorrer na crítica de Tullio Ascarelli (2008, p. 35) ao direito comparado: "O que cumpre estudar é o direito comparado e não simplesmente a legislação comparada, a menos que se queira correr o risco de tirar conclusões que, pelo fato de não serem completas, poderiam ser, afinal, erradas".

Em verdade, o direito à autodeterminação informativa na modernidade parece um viés do direito à privacidade, uma ampliação do seu núcleo, algo que participa de sua própria definição. A exemplo da legislação brasileira, o único momento em que o direito em comento é citado deu-se na LGPD[62], trazendo-o como fundamento da proteção dos dados pessoais.

A noção geral de um usuário da internet é que haveria um autocontrole no compartilhamento de suas informações, eis que ele escolhe o que divulgar em suas redes sociais ou o que compartilhar com os sites que acessa. Contudo, mesmo após essa escolha do compartilhamento, é necessário ter controle de quais informações derivaram das informações concedidas. De forma mais precisa, são necessários o controle e o acesso aos perfis comportamentais criados com base na atuação do indivíduo na rede.

Assim, é imprescindível notar que o direito à privacidade cada vez se vincula menos à "secretividade" das informações, ligando-se mais for-

dade, o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações." (DONEDA, 2006, p. 197)

61 Tradução livre. "*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*". (WESTIN, 1967, p. 7.)

62 Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II – a autodeterminação informativa.

temente ao controle da pessoa sobre dados de sua titularidade (BLUM, 2018, p. 27).

O compartilhamento e detalhamento da vida pessoal para quem quer que possua interesse, em verdade, já virou o *métier* de milhares de pessoas, autodenominadas digitais *influencers*, de forma que as características originárias do direito à privacidade cedem lugar ao foco na proteção contra o uso indevido de dados pessoais. Para Byung-Chul Han, a exposição da intimidade nas mídias sociais faz o privado se tornar público:

> A falta de distância leva a que o privado e o público se misturem. A comunicação digital fornece essa exposição pornográfica da intimidade e da esfera privada. Também as redes sociais se mostram como espaços de exposição do privado. A mídia digital como tal *privatiza* a comunicação, ao deslocar a produção de informação do público para o privado (grifos do autor). (HAN, 2018)

Elucida Sérgio Branco (2017, p. 137) que "[d]esde o começo dos tempos, esquecer tem sido a regra e lembrar, a exceção". Porém, hoje, o direito ao esquecimento ou à desindexação é cada vez mais posto em xeque, ante a amplitude e a inesgotabilidade de caminhos que a informação pode percorrer.

A construção do direito à autodeterminação informativa foi essencial ao estabelecimento do direito à privacidade, que amplia seu conteúdo ao direito à privacidade informacional e dele participa. Não se pode mais aceitar que a relação entre a sociedade e a tecnologia se dê como uma caixa-preta em que pouco se sabe sobre as informações que armazena.

2.4 O superdimensionamento do consentimento

A inserção das tecnologias digitais mudou a forma de interação humana, mas, principalmente, aumentou a velocidade das mudanças sociais. O trabalho do jurista se torna mais complexo, pois estratificar toda a informação social em tratamento legal ou principiológico, além da escolha do que não será regulado, tornou-se tarefa hercúlea. Assim, ao estar diante da contraditória imutável evolução das tecnologias, tal trabalho deve ser

realizado pautando-se, principalmente, na proteção da pessoa como valor máximo do ordenamento (DONEDA, 2006, p. 34).

Nesse contexto, é necessária a análise da transformação do consentimento em pseudoconsentimento nos negócios digitais, como forma de compreender a sua importância para a abertura do direito à privacidade do indivíduo àquele que se consente.

O consentimento é figura central para a matéria jurídica. É a partir dela que se estabelecem parâmetros de conduta e eventuais responsabilizações de agentes. A forma em que o consentimento se concretiza também é relevantíssima. Este, para sua validade formal, deve ser exteriorizado de forma inequívoca, exceto quando a lei dispõe sobre a sua prescindibilidade.

Quem cala, consente?

A palavra consentir "sugere ideia de 'permitir, de não discordar, qualquer que seja o motivo do consentimento'" (POMBO, 2011, p. 72). Contudo, o "não discordar" implica em uma atitude passiva daquele que consente. A figura do consentimento no direito à proteção de dados pessoais, implica, por sua vez, em uma ação por parte do indivíduo, já que o consentimento possui implicações que podem ir além o seu conhecimento.

O ditado "Quem cala, consente" poderia ser reescrito na sociedade informacional como "Quem clica, consente". Deve-se ter olhos de desconfiança a quem quer que afirme que jamais aceitou um Termos de Uso ou uma Política de Privacidade sem ler.[63] Isto porque o *e-mail* que acessa, o sistema operacional do computador e do celular e até a *smart* TV que adquire possuem páginas e mais páginas de cláusulas pouco acessíveis e não personalizáveis.[64]

Ao tratar das premissas teóricas da legitimação do poder estatal fundado no consentimento, George Marmelstein afirma que este "é construído a partir da crença de que o ser humano é um ser reflexivo que, em dadas circunstâncias, pode agir em conformidade com o projeto de vida

63 Nesse sentido, Stefano Rodotà destaca que houve o gradual abandono da técnica do *implied consent*, em virtude das especificações mais analíticas, destacando-se o *informed consent*, que prescreve quais informações devem ser fornecidas pelo interessado para que seu consentimento seja considerado válido. (RODOTÀ, 2008, p. 75)

64 Cf. a interessante história criada por Bruno Bioni sobre a vida cerceada por termos de uso. (BIONI, 2019. p. 23-24)

que escolheu para si" (MARMELSTEIN, 2018, p. 70). Mesmo que o consentimento aqui tratado não seja o político ou o ético-jurídico, o ato de consentir deve ser necessariamente reflexivo, se há qualquer pretensão de espelhamento deste no mundo jurídico. O autor continua: "A ideia de consentimento está ligada à necessidade de justificação das decisões tomadas" (IDEM, p. 183).

Adotar o paradigma do consentimento insere-se na ideia do homem como indivíduo racional e capaz de refletir sobre seus atos. Bruno Bioni (2019, p. 136) aduz que esse papel de protagonista se iniciou na segunda geração de leis sobre a proteção de dados pessoais, sendo estratégia regulatória em que se depositava no indivíduo a responsabilidade de autoproteger suas informações pessoais. Laura Schertel amplia ainda este entendimento para além da segunda geração de leis de proteção de dados pessoais, mas também a terceira geração, em que buscavam estabelecer a participação do indivíduo no processo de tratamento de dados. Contudo, "os altos custos monetários e sociais que os cidadãos deveriam suportar para exercer seus direitos tornaram essa participação ilusória" (MENDES, 2014, p. 61).

Na ideia inicialmente introduzida por Herbert Simon (1955), há a proposição de substituição do homem racional e econômico pelo homem com habilidades e conhecimentos limitados.[65] Tal proposição, facilmente aceita nos dias de hoje, precisou ser introduzida doutrinariamente para a sua completa aceitação. Na definição de Christine Jolls, Cass R. Sunstein e Richard Thaler, como expressão da racionalidade limitada (*bounded racionality*):

> Nós temos habilidades computacionais limitadas e memórias seriamente falhas. As pessoas podem responder sensatamente a essas falhas; assim, pode-se dizer que elas às vezes respondem racionalmente às suas próprias limitações cognitivas, minimizando a soma custos de decisão e custos de erro. Para lidar com memórias limitadas, fazemos listas. Para lidar com o

65 Nas palavras do autor: "*The paradox vanishes, and the outlines of theory begin to emerge when we substitute for "economic man" or "administrative man" a choosing organism of limited knowledge and ability. This organism's simplifications of the real world for purposes of choice introduce discrepancies between the simplified model and the reality; and these discrepancies, in turn, serve to explain many of the phenomena of organizational behavior*". (SIMON, v. 69, n. 1. p. 99-118)

> poder e o tempo limitados do cérebro, usamos atalhos mentais e regras do polegar.[66]

A racionalidade limitada inerente ao homem, portanto, dificulta que sejam a ele imputados aspectos significativos de decisão quando, sabiamente, o que se dispõe ao consentir com o tratamento de dados pessoais não é a análise por outro humano igualmente limitado, mas sim por máquinas capazes de um autoaperfeiçoamento.

Bruno Bioni destaca, ainda, que há barreiras psicológicas capazes de mistificar a capacidade do indivíduo em controlar as suas informações pessoais. A primeira delas é chamada de teoria da utilidade subjetiva, em que "O ser humano tem a tendência de focar nos *benefícios imediatos*, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço *on-line*" (grifos do autor). (BIONI, 2019, p. 147)

Assim, nessa teoria destaca-se a falta de sopesamento dos prejuízos à privacidade, eis que estes apenas advirão em um futuro incerto. Outra teoria significativa é a teoria prospectiva, em que "o processo da tomada de decisão tende a se levar pelo contexto de que as perdas são maiores que os ganhos" (IDEM, p. 147-148). Ela parte da premissa de que o custo para retomar o controle dos próprios dados pessoais é visto como uma perda, enquanto o ganho seria o acesso imediato ao serviço.

Nesta teoria vislumbra-se a própria dificuldade que o indivíduo enfrenta para visualizar as consequências do seu consentimento imediato em um ambiente de clara assimetria da informação. Para Laura Schertel (2014, p. 65), "[...] nem sempre é possível ao indivíduo dimensionar as consequências futuras de uma disposição em relação aos seus dados".

66 Tradução livre: "*We have limited computational skills and seriously flawed memories. People can respond sensibly to these failings; thus it might be said that people sometimes respond rationally to their own cognitive limitations, minimizing the sum of decision costs and error costs. To deal with limited memories we make lists. To deal with limited brain power and time we use mental shortcuts and rules of thumb*". JOLLS, Christine; SUNSTEIN, Cass R.; THALER, Richard. A Behavioral Approach to Law and Economics. **Stanford Law Review**, [s.l.], v. 50, n. 5. p.1471-1550, maio 1998. JSTOR. http://dx.doi.org/10.2307/1229304. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12172&context=journal_articles>. Acesso em: 14 jun. 2019.

Shoshana Zuboff trata a questão da assimetria de informação de forma ainda mais profunda, de maneira que muitas das operações de tratamento de dados hoje são desenhadas para serem invisíveis aos indivíduos:

> O capitalismo de vigilância opera por meio de assimetrias sem precedentes no conhecimento e do poder que se acumula no conhecimento. Os capitalistas de vigilância sabem tudo sobre nós, enquanto suas operações são projetadas para serem desconhecidas para nós. Eles acumulam vastos domínios de novos conhecimentos de nós, mas não para nós.[67]

Essas teorias se vinculam fortemente à teorização da sociedade de cansaço, de Byung-Chul Han. Há um problema de consentimento na era do cansaço. Para o autor, "o próprio senhor se transformou num escravo do trabalho" (HAN, 2018, p. 47). Essa escravidão moderna leva a uma sociedade de desempenho que exige do indivíduo cada vez mais.[68] Este indivíduo amplamente exigido, sem qualquer descanso, continuamente conectado, não pode ser tomado como ter um consentimento verdadeiramente livre.

Para a proteção do usuário na internet, é imprescindível uma definição completa do consentimento que fosse capaz de abranger e proteger as relações que se firmam no ambiente da rede mundial. Essa tentativa de abranger o consentimento iniciou na Diretiva Europeia 95/46/CE, que em seu art. 2º, alínea h, aduzia: "'Consentimento da pessoa em causa', qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam

67 Tradução livre: "*Surveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge. Surveillance capitalists know everything about us, whereas their operations are designed to be unknowable to us. They accumulate vast domains of new knowledge from us, but not for us*". ZUBOFF, Shoshana. **The age of Surveillance Capitalism:** The fight for a human future at the new frontier power. E-book Kindle. Nova Iorque: Public Affairs, 2019, Capítulo 1, tópico III, paginação irregular.

68 Nesse sentido, aponta Byung-Chul (2018, p. 47): "E visto que, em última instância, está concorrendo consigo mesmo, procura superar a si mesmo até sucumbir. Sofre um colapso psíquico, que se chama de burnout (esgotamento". O sujeito do desempenho se realiza na morte. Realizar-se e autodestruir-se, aqui, coincidem".

objecto de tratamento".[69]

Por sua vez o Regulamento Geral de Proteção de Dados Pessoais[70] de 2016, do Parlamento Europeu e Conselho da União Europeia, que revogou a diretiva, dispõe em art. 4º, 11: "'Consentimento' do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".[71]

Ainda nas considerações iniciais do regulamento, precisamente no item 32, o consentimento pode ser dado validando uma opção ao visitar um sítio *web* na internet, mas o silêncio, por si só, não constitui o consentimento.[72]

Da diretiva ao regulamento, houve o acréscimo da "expliciticidade" do consentimento, de forma que esta manifestação deve ser inequívoca, retomando a um aprimoramento do conceito, que não mais seria um mero "quem clica, consente".

A LGPD, por exemplo, adotou o consentimento como uma de suas bases legais em seu art. 7º, não sendo a única base sobre a qual o tratamento de dados pode ser realizado.[73] Apesar de não existir hierarquia entre estas,

69 PARLAMENTO EUROPEU, CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046> Acesso em: 15 jun. 2019.

70 Mais amplamente conhecido como General Data Protection Regulation – GDPR.

71 PARLAMENTO EUROPEU, CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.** Disponível em: <https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32016R0679> Acesso em: 15 jun. 2019.

72 Idem, ibidem.

73 No art. 7º da LGPD foram elencadas dez bases legais em seus incisos, sendo elas: Consentimento, Cumprimento de obrigação legal, Execução de políticas públicas, Estudos por órgão de pesquisa, Execução de contratos ou diligências pré-contratuais, Exercício regular de direitos, Proteção da vida, Tutela da saúde, Interesses legítimos do controlados ou terceiro e Proteção de crédito.

na referida lei, a referência ao consentimento é superdimensionada em relação às outras bases legais, sendo citada 35 (trinta e cinco) vezes dos seus mais de 65 (sessenta e cinco) artigos. Na LGPD, seguindo as legislações de dados pessoais modernas, há uma veneração do consentimento.[74]

A atual definição brasileira de consentimento elencada na Lei Geral de Dados Pessoais baseou-se mais na Diretiva 95/46/CE do que no Regulamento que a revogou. Nos termos da lei, consentimento é "manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma **finalidade determinada**" (grifos nossos).[75]

Diferentemente do regulamento europeu, que optou pelos termos explícito e específico para o consentimento de quaisquer dados pessoais, a lei brasileira designou tais termos apenas para o tratamento de dados pessoais sensíveis, no teor do art. 11, inciso I: "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

Após tais considerações, passa-se a uma análise dos elementos centrais definidos pela lei brasileira.

2.4.1 Livre

O consentimento livre é uma escolha real e significativa? A pessoa poderia consentir? A perspectiva de liberdade na sociedade de vigilância é propagada juntamente com a ideia de transparência e com ela se confunde. O ser humano é livre para viver em isolamento, mas, a partir do momento em que escolhe inserir-se no meio digital, inicia-se uma liberdade condicional. É livre, mas deve estar sempre comunicável por meio de aparelhos celulares. É livre, mas só pode submeter-se a certo serviço se aceitar os termos irretocáveis que ele carrega.

74 À exemplo de Bruno Bioni (2019, p. 26), que aduz que o consentimento continua a ser venerado na atualidade.

75 Art. 5º Para os fins desta Lei, considera-se: [...] XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

A digitalização da vida é cada vez mais iminente, tanto que a Assembleia Geral das Nações Unidas já definiu a importância social da internet da seguinte forma:

> De fato, a Internet se transformou em uma das principais formas por meio das quais os indivíduos podem exercitar seus direitos à liberdade de opinião e expressão, como garantido pelo artigo 19 da Declaração Universal de Direitos Humanos e o Pacto Internacional de Direitos Civis e Políticos.[76]

A liberdade na rede mundial de computadores, contudo, fica restringida a partir do momento em que a principal forma de acesso a ela se dá por meio das detentoras dos reinados tecnológicos invisíveis. Ou seja, há o paradoxo da liberdade, até possuindo direito ao acesso à internet, mas este é invariavelmente interrompido por termos e políticas de privacidades dos principais provedores, navegadores e sites que os usuários médios utilizam. Este seria um paradoxo da liberdade.

Danilo Doneda aponta, ainda, o paradoxo da privacidade, em que aquele que consente apenas poderá obter alguma proteção após o consentimento ser realizado, implicando que primeiro a pessoa consente em dispor de seus dados para em seguida valer-se de tutela de proteção dos dados pessoais. Para o autor, portanto, o consentimento com tais características seria uma ficção. O consentimento não poderia ser utilizado para neutralizar a atuação dos direitos fundamentais, já que o perfil do consentimento na disciplina dos dados pessoais não se embasa na atuação da autonomia privada em mecanismos negociais tradicionais.

O aprofundamento da liberdade do homem na sociedade e os limites desta passa a questões filosóficas que transcendem os objetivos deste trabalho, mas desde já se ressalva que em relações que implicam su-

76 Tradução livre. "*Indeed, the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights*". ORGANIZAÇÃO DAS NAÇÕES UNIDAS – ONU. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.** 2011. Disponível em: <https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. Acesso em: 15 jun. 2019.

bordinação, como as de trabalho ou consumeristas, o consentimento não seria verdadeiramente uma manifestação livre.[77]

No tocante à liberdade, a verificação desta é nebulosa quando se trata, ainda, dos hipervulneráveis. Entre estes se encontram os idosos e os absolutamente incapazes. Em verdade, qualquer questão de desenvolvimento neurológico incompleto ou defasado infere na liberdade da pessoa em proferir um consentimento.

A inserção de crianças e adolescentes no meio digital ocorre de forma cada vez mais precoce, não sendo incomum que bebês saibam utilizar uma *touchscreen*, ou que crianças de aproximadamente 5 anos já tenham seu próprio *tablet* com capinhas de borracha coloridas. Em verdade, os novos aparelhos são programados com uma interface tão intuitiva que facilita a manipulação em todas as idades. No entanto, é válida e necessária a ressalva de Pedro Hartung et al. em que: "[...] indivíduos de até 12 anos de idade incompletos e entre 12 e 18 anos de idade, respectivamente – foram reconhecidos como pessoas em um processo peculiar e inconcluso de desenvolvimento biológico, cognitivo e emocional [...]" (HARTUNG, 2017, p. 160-184).

Para Laura Schertel, quanto aos hipervulneráveis, as normas aplicáveis aos negócios jurídicos para demonstração do consentimento podem ser aplicadas ao tratamento de dados pessoais com reserva. Para a autora, uma norma não aplicável para aferição do consentimento é o da capacidade civil, estabelecida nos arts. 3º e 4º do Código Civil.[78] Nesse caso:

> o caráter personalíssimo do consentimento para o processamento de dados pessoais: fundamental é identificar se a pessoa tem

77 O tratamento de dados de empregados é questão sensível, mas, tendo em vista a dificuldade do consentimento ser aplicável a esta modalidade, a base legal do inciso V, do art. 7º da LGPD, da possibilidade de tratamento para a execução de contrato, é a mais adequada às relações trabalhistas.

78 Art. 3º São absolutamente incapazes de exercer pessoalmente os atos da vida civil os menores de 16 (dezesseis) anos.
Art. 4º São incapazes, relativamente a certos atos ou à maneira de os exercer: I – os maiores de dezesseis e menores de dezoito anos; II – os ébrios habituais e os viciados em tóxico; III – aqueles que, por causa transitória ou permanente, não puderem exprimir sua vontade; IV – os pródigos. Parágrafo único. A capacidade dos indígenas será regulada por legislação especial.

> capacidade de discernimento (*Einsichtsfähigkeit*) para autorizar determinado tipo de coleta ou tratamento de dados, não sendo necessária a capacidade civil para tanto (MENDES, 2014, p. 63).

A autora aduz, ainda, que a autoridade de proteção de dados alemã identifica que a partir de 14 (quatorze) anos a pessoa já poderia consentir com o tratamento de dados pessoais. Vale notar que o RGPD, em seu art. 8º, destaca a possibilidade de disposição da matéria pelos Estados membros, desde que a idade não seja inferior a 13 (treze) anos:

> Artigo 8º
>
> Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação
>
> 1. Quando for aplicável o artigo 6º, n. 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.
>
> Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.
>
> 2. Nesses casos, o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível.
>
> 3. O disposto no n. 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança.[79]

79 PARLAMENTO EUROPEU, CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais**

A lei brasileira regulou a matéria concernente ao consentimento de absolutamente e relativamente incapazes para o tratamento de dados pessoais no sentido que o consentimento deverá ser específico e em destaque, dado por pelo menos um dos pais ou responsável legal (Art. 14, §1º). Ainda, "o controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis".[80]

Assim, em vez de regular a idade em que o consentimento poderia ser dado pelos hipervulneráveis, destacou-se que este deverá ser dado por, pelo menos, um dos pais. Não se sabe até quando isto seria factível, eis que a partir de certa idade, principalmente entre os adolescentes, a depender da forma que esse consentimento dos pais seja exigido, não passaria de uma ficção jurídica.

Como em muitos casos esse consentimento se confunde com a própria possibilidade de acessar determinados provedores, aplicativos e conteúdos, não se poderia impor que pré-adolescentes se tornem eremitas do acesso à rede, já que internet é aspecto central e indispensável da vida moderna e, inclusive, da própria formação do ser humano do século XXI.

Contudo, considerar o consentimento como válido de pessoa considerada na legislação civil absolutamente incapaz é ir contra toda a construção da capacidade civil nos negócios jurídicos que também devem ser aplicadas nos negócios *on-line*.

Portanto, a utilização da rede pelo absolutamente incapaz cabe ao tutor ou curador, devendo o consentimento ser por ele realizado. No caso de consentimento para dados pessoais dado por absolutamente incapaz, deve ser considerado nulo, nos termos do art. 166, inciso I do Código Civil.[81]

Também, mesmo que se impere um saudosismo sobre as brincadeiras na rua, sem crianças vidradas em televisões ou videogames, é fato que não se pode regredir na digitalização e virtualização de crianças e

e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32016R0679> Acesso em: 15 jun. 2019.

80 Art. 14, § 5º, LGPD.

81 Art. 166. É nulo o negócio jurídico quando: I – celebrado por pessoa absolutamente incapaz;

adolescentes, sob pena de causar uma evidente exclusão social no círculo de convivência destas.

2.4.2 Informado

A medida de um consentimento informado inserido na perspectiva de uma racionalidade limitada humana é questionável. Estar informado seria saber o que se está consentindo enquanto titular e ainda receber as informações de maneira clara, direta e concisa. Alia-se ao princípio da informação, que consoante Danilo Doneda: "refere-se a uma completa consciência do interessado sobre o destino de seus dados pessoais caso este forneça o consentimento para o tratamento" (DONEDA, 2006, p. 383). Ainda, um consentimento informado implica em um caráter de subjetividade difícil de ser aliado à uma medida se este foi ou não suficientemente informado.

O critério sobre um consentimento informado muda drasticamente com o nível de escolaridade do agente que consente. O Brasil, que possui população projetada de 210.059.953 milhões de pessoas[82] em 2019, tem 7,2% da população sem qualquer instrução ou menos de 1 ano de estudo, 8% da população com ensino fundamental ou equivalente, 24,4% da população com ensino médio completo ou equivalente e 12,7% com ensino superior completo ou equivalente, consoante análise de dados do primeiro trimestre de 2019.[83]

Com uma distribuição de escolaridade tão desigual, avaliar se o consentimento foi realmente informado depende da análise casuística do perfil do titular. A compreensão por alguém do que implica autorizar o tratamento de dados pessoais possui grande amplitude no Brasil, sendo de difícil resolução aplicar uma fórmula da qual se depreenda de cada usuário se a informação foi devidamente compreendida.

A sociedade informacional possibilita o acesso à informação de forma rápida e fácil. A qualidade de tal informação, no entanto, é questionável.

82 Dados consultados em 17 de junho de 2019, às 14:26, com atualização em tempo real. IBGE. Projeção da população do Brasil e das Unidades da Federação. Disponível em: <https://www.ibge.gov.br/ap ps/populacao/projecao/> Acesso em: 17 jun. 19.

83 IBGE. Tabela 5919 – População por níveis de instrução. Disponível em: <https://sidra.ibge.gov.br/ tabela/5919#resultado> Acesso em: 17 jun. 19.

Há a supervalorização de sites como Wikipedia, que é editado por qualquer pessoa que não necessariamente o faz de boa-fé ou com cientificidade. Ou seja, há abundante fonte de informação sem a necessária confiança sobre sua origem para sua utilização.

Como caso prático da impossibilidade de emitir um consentimento informado, em janeiro de 2019, o *Google* foi multado em 50.000.000,00€ (cinquenta milhões de euros) pela autoridade francesa de proteção de dados, *Commission Nationale de l'informatique et des Libertés* (CNIL), após uma queixa coletiva com mais de dez mil signatários, em que alegavam falta de transparência, de consentimento válido e de informações insuficientes para a personalização de publicidade, já que o consentimento era obtido por blocos de finalidades, sem a possibilidade real de ajuste ou alteração.[84] Destaque-se que na Lei Geral de Proteção de Dados brasileira foi instituído o limite máximo de multa como R$ 50.000.000,00 (cinquenta milhões de reais).

2.4.3 Inequívoco

O espectro do consentimento como inequívoco o requer que seja demonstrável por meio de prova. Para isso, as empresas utilizam-se de cliques para obter o consentimento como inequívoco e alguns aplicativos de instituições financeiras ou corretoras de valores empregam a impres-

84 Relativa à forma que o consentimento era exigido pela empresa, considerada abusiva pela autoridade, a decisão contém: "*Par exemple, s'agissant des traitements de personnalisation de la publicité, pour connaitre les informations qui sont collectées auprès de lui pour cette finalité, un utilisateur* ***doit accomplir de nombreuses actions et combiner plusieurs ressources documentaires****. Dans un premier temps, il doit prendre connaissance du document général Règles de confidentialité et conditions d'utilisation , puis cliquer sur le bouton Plus d'options et ensuite sur le lien En savoir plus pour que soit affichée la page Personnalisation des annonces.* ***Il aura ainsi accès à une première description du traitement relatif à la personnalisation de la publicité qui s'avère être incomplète****. Pour compléter l'information relative aux données traitées dans le cadre de cette finalité, l'utilisateur devra encore consulter dans son intégralité la rubrique proposer des services personnalisés contenue dans le document Règles de confidentialité, lui-même accessible depuis le document général Règles de confidentialité et conditions d'utilisation*". (grifos nossos) COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Délibération n. SAN-2019-001 du 21 janvier 2019: Délibération de la formation restreinte n. SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC**. 2019. Disponível em: <https://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000038032552>. Acesso em: 14 jun. 2019.

são digital para verificar a autenticidade daquele que está consentindo, conforme a existência ou não dessa funcionalidade em aparelho celular do indivíduo. A questão está pormenorizadamente tratada no item 2.4.5 – Alcance jurídico do "Li e Aceito" e suas consequências para o usuário.

2.4.4 Finalidade determinada

Por fim, há o requisito do tratamento dos dados pessoais com uma finalidade determinada. Há uma pretensão de encerrar o consentimento amplo que, por exemplo, ao consentir com o tratamento de dados pessoais pela empresa fabricante de uma pulseira que calcula os quilômetros percorridos em uma corrida, o mesmo sistema da pulseira poderia tratar tais dados para verificar o endereço da casa, do trabalho e as rotas de preferência do usuário. De forma mais obscura, o sistema operacional poderia até mesmo fazer verificações do estado de saúde do usuário que seriam indevidamente vendidos às seguradoras. Com isso, a inserção de uma finalidade determinada busca que o tratamento consentido ocorra apenas naqueles casos alinhados com a expectativa do titular.

A colocação do princípio da finalidade na própria definição de consentimento sugere evitar a tentativa de obter um consentimento geral para o tratamento de dados (DONEDA, 2006, p. 383). Aparentemente, buscou o legislador inserir ditames da base legal do legítimo interesse, preconizada no art. 7º, inciso IX[85] da LGPD, na definição da base legal do consentimento.

Como visto, a figura do consentimento, que por muitas gerações das leis de proteção de dados pessoais era vista como principal forma de controle dos dados pelo titular, passou a ter rígidos critérios que quiçá inviabilizem a sua concreta utilização nos negócios imediatos do meio digital. De acordo com Marcel Leonardi, na Europa, após a vigência do RGPD, o consentimento passou a ser um dos métodos de tratamentos de dados pessoais menos utilizados por conta de suas sucessões de exigências, sendo a base legal do legítimo interesse utilizada em até 70% dos trata-

85 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; [...]

mentos de dados pessoais em detrimento do consentimento.[86]

A revogação do consentimento é outra questão que passou apenas a ser modernamente tratada. Ela parte da premissa de que ao consentir deve-se haver a necessária possibilidade de revogar o consentimento dado. Caso contrário, um consentimento poderia ser visto como algo vitalício, que perduraria enquanto a existência do indivíduo.

Tal revogação é importante pois antes, em caso de violação do direito à privacidade ou excessos no tratamento de dados pessoais, o titular não poderia buscar uma reparação da violação, já que, por haver consentido, deveria arcar com suas consequências (MENDES, 2014, p. 42-43).

Para Laura Schertel, a possibilidade de revogação do consentimento é prerrogativa "fundamental para fazer valer a autodeterminação do indivíduo e o livre desenvolvimento de sua personalidade" (IDEM, p. 63). Continua, aduzindo que além da revogação constituir parte do direito à autodeterminação informativa, é necessária tendo em vista a proteção de dados pessoais como um direito da personalidade (IDEM, p. 64). Assim, a ideia de revogabilidade incondicional do consentimento estaria aliada na proteção da própria personalidade, mas poderia apresentar dificuldades de aplicação prática (DONEDA, 2006, p. 380). Tal teorização foi abrangida pela LGPD, que em seu art. 8º, § 5º contém:

> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

Ademais, a Lei dispõe sobre possibilidades de revogação caso: a finalidade, a forma, a duração ou o controlador do tratamento sejam alterados (art. 8º, § 6º, repetido em parte pelo art. 9º, § 2º), por mera comunicação do titular dos dados para término do tratamento dos dados (art.

86 LEONARDI, Marcel. A empresa e a proteção de dados (Lei n. 13.709/18), 28:05 – 28:10 minutos. *In*: IX Congresso Brasileiro de Direito Comercial. São Paulo, 2019. Disponível em: <https://www.congressodireito comercial.org.br/site/direito-do-comercio-eletronico-8> Acesso em: 17 jun. 19.

15, III), dispondo ainda que o titular tem direito a obter do controlador a revogação do consentimento (art. 18, IX).

Como se vê, a figura do consentimento surgida nas primeiras gerações de leis de dados pessoais evoluiu a um pseudoconsentimento no século XXI. Hoje, para evitar-se tal pseudoconsentimento, o consentimento foi seriamente regulado pelas atuais disposições sobre o tratamento de dados pessoais, o que criou dificuldades à sua aplicabilidade. O que se verifica, com isso, é a falta de aptidão do conceito, em qualquer auge de regulação, para a proteção do direito à privacidade informacional.

Ante a autorização legal que o tratamento de dados pessoais se dê em outras hipóteses definidas pela lei, além do consentimento, o que se espera é uma diminuição em sua atuação para pautar os negócios *on-line*. Apesar disto, enquanto se vê um consentimento hiperregulado, as demais bases legais são precariamente tratadas, restando, assim, um controle de legalidade sobre sua aplicação prática pela Autoridade Nacional de Proteção de Dados.

Realizadas as considerações gerais acerca do consentimento, discute-se os limites da utilização de dados pessoais no ambiente digital, partindo do futuro das cláusulas de "Li e Aceito", bem como do tratamento específico que deve se aplicar aos Termos de Uso e Políticas de Privacidade.

2.4.5 Alcance jurídico do "Li e Aceito" e suas consequências para o usuário

Parafraseando o texto bíblico para a temática: "Quem de vós estiver sem pecado, seja o primeiro a lhe atirar uma pedra".[87] Efetivamente, trata-se de tarefa hercúlea encontrar indivíduo que leu todos os "Termos de Uso e Políticas de Privacidade" antes de expressar o seu consentimento, supostamente informado, no clique na cláusula "Li e Aceito".

Muitas vezes escrita de diferentes formas quando apresentada nos computadores *desktop*, "Li e Concordo", "Afirmo que Li e Aceito", entre outras variações, incluem a mesma carga de responsabilidade. Em regra, afirma-se que leu e concordou com o tratamento de dados pessoais, com a

87 Evangelho de João, capítulo 8, versículo 7.

criação de perfis comportamentais, com o direcionamento de publicidade e, em casos extremos, como a antiga política de privacidade do *Facebook*, que consente na exploração de perfis dos amigos na rede social.

Ainda, ante a massiva utilização de *smartphones* e aplicativos para melhorar a experiência do usuário, uma tentativa de se obter o consentimento se dá por um rápido clique nos termos "Ok", "Aceito" e "Confirmo".

Efetivamente, dada a pressa vivenciada no mundo virtual, em que não se há tempo a perder para usufruir das facilidades da vida digital, um rápido clique não pode ser comparado *à uma formal assinatura contratual na vida real*.[88]

Perceber a carga informacional de um mero clique é difícil tarefa. As pessoas dão cliques e duplos cliques para qualquer coisa. É um meio de interagir e se relacionar na vida social. Ressalte-se que com os aparelhos *touchscreen*, os cliques estão no limite do obsoleto, sendo substituídos por toques e leituras de digitais.

Um exemplo da ausência de reflexão dos cliques dos usuários está na experiência do jogo do *Facebook, Cow Clicker*. Como uma crítica aos famosos jogos de fazendinha da rede social, Ian Bogost criou um jogo em que se clicava em imagens de vacas e, como recompensa, os jogadores recebiam um mugido e um "clique", o dinheiro digital do jogo, que poderia ser trocado por novos modelos de vacas.

88 O que é real? Hoje, muitas vezes a vida mais se transpõe ao meio digital que nada impede que esta seja vista como a real vida que se possui. Afinal, é lá que estão os perfis sociais, as centenas de amigos e os perfis criados, com múltiplas possibilidades de interação.

FIGURA 5 – MODELOS DE VACAS DO JOGO COW CLICKER

Fonte: BOGOST, Ian. My Cow Game Extracted Your Facebook Data. The Atlantic 2018. Disponível em: <https://www.theatlantic.com/technology/archive/2018/03/my-cow-game--extracted-your-facebook-data/556214/> Acesso em: 19 jun. 2019

O criador do jogo assumiu que, com a rápida autorização obtida pelos usuários ao jogar, era capaz de captar dados preciosos:

> [...] se você jogou Cow Clicker, mesmo apenas uma vez, eu recebi o suficiente de seus dados pessoais que, por anos, eu poderia ter reunido um perfil razoavelmente sofisticado de seus interesses e comportamento. Eu ainda posso ser capaz disso; todos os dados ainda estão lá, armazenados no meu servidor privado, onde Cow Clicker ainda está em execução, permitindo que os jogadores continuem clicando onde uma vez esteve uma vaca, antes que meu capricho os arrebatasse para o vazio digital.[89]

89 Tradução livre: "[…] *if you played Cow Clicker, even just once, I got enough of your personal data that, for years, I could have assembled a reasonably sophisticated profile of your interests and behavior. I might still be able to; all the data is still there, stored on my private server, where Cow Clicker is still running, allowing players to keep clicking where a cow once stood, before my caprice raptured them into the digital void*". BOGOST, Ian. My Cow Game Extracted Your Facebook Data. **The Atlantic**. 2018. Disponível em: <https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/5562 14/> Acesso

Percebe-se, assim, o esvaziamento da dimensão de um clique. A partir deste, não há real visualização da expectativa do titular. *É* indispensável que, ao se utilizar de um clique para o tratamento de dados pessoais, seja levada em consideração a expectativa daquele. No jogo *Cow Clicker*, a expectativa era apenas jogar de forma satírica, clicando em uma vaca que mugia. Apesar de não haver qualquer perspectiva de consentimento para o tratamento de dados pessoais pelo usuário, houve a coleta indiscriminada de dados nos mesmos parâmetros da coleta do vazamento de dados da *Cambridge Analytica*.

Neste mercado em que o principal insumo são os dados pessoais, há um assédio de consumo em que quase tudo, por girar em torno das informações do usuário, exige um pseudoconsentimento com base em um clique de "Li e Aceito".

Nesse assédio, incluem-se aquelas ferramentas que, utilizando-se de um propósito, acrescentam em seus termos a personalização de publicidade. Utilize-se como exemplo, mais uma vez, o aplicativo de conversas instantâneas *WhatsApp*.[90] Apesar de constar em sua política de privacidade que: "Nós continuamos a não permitir banners com anúncio de terceiros no *WhatsApp*", logo em seguida consta:

> Nós iremos explorar maneiras para que você possa **se comunicar com empresas através do WhatsApp**, interações como pedidos, transações, informações sobre consultas, alertas para entrega de pedidos, **atualizações sobre produtos e serviços e marketing**. Por exemplo, você poderá receber notificações sobre o status do voo de sua viagem, um recibo de uma compra que você tenha feito, ou uma notificação assim que uma entrega tenha sido feita. **Mensagens de marketing que você venha a receber, poderão conter ofertas de algo que lhe interesse**. (grifos nossos).[91]

em: 19 jun. 2019.

90 Aplicativo escolhido pela alta penetração no cotidiano dos brasileiros.

91 WHATSAPP. **Informação Legal do Whatsapp**. Disponível em: <https://www.whatsapp.com/legal/?lang=pt_ br#privacy-shield> Acesso em: 19 jun. 2019.

No item "Atualizações Importantes", destaca que a partir de 2014 o aplicativo foi comprado pelo *Facebook* e que, para melhorar seus produtos e ofertas podem "como por exemplo, combater *spam* entre os aplicativos, dar sugestões sobre o produto, mostrar anúncios relevantes entre outros no *Facebook*". Ou seja, o aplicativo, totalmente gratuito, utiliza-se das conversas de milhões de brasileiros para personalizar anúncios relevantes em empresa diferente da qual se foi coletada a informação.

Isso explica a compra do aplicativo pelo *Facebook* por US$ 22 bilhões em 2014.[92] *Não há plataforma melhor para estudo comportamental dos indivíduos e direcionamento de publicidade.* No mesmo sentido pode ser vista a compra do aplicativo de reconhecimento de música *Shazam* pela *Apple*. Estima-se que a aquisição se deu por US$ 400 milhões em 2018. Como consequência da aquisição, ainda tornou o aplicativo completamente livre de anúncios, excluindo a possibilidade de pagar por essa funcionalidade.[93]

Destaque-se que o *Shazam* possui um sistema com amplo reconhecimento de voz e a capacidade de compará-la em seus numerosos dados de música para encontrar o que o usuário deseja. Esta tecnologia, apesar de ter grande utilidade em alguns aspectos, força a reflexão de que os aparelhos celulares são, cada vez mais, formas intermitentes de vigilância do comportamento do usuário para fins publicitários.

Ao clicar o "Li e Aceito" ou "Ok" para a captura de sons do ambiente, implica também que o aparelho está de forma intermitente ouvindo o indivíduo. Por isso a sensação de que a publicidade hoje lê a mente das pessoas. Em verdade, consoante "Termos de Uso do *WhatsApp*" e de outros grupos de empresas, há o compartilhamento de informações entre o grupo, não sendo incomum algo que se digita ou fala apareça como publicidade em uma mídia diferente.

*É problemátic*a ainda a utilização de verbos nos "Termos de Uso" que indiquem como os dados poderão ser usados de forma exemplificativa, e *não de forma restritiva.* Mais uma vez, a exemplo dos termos do *WhatsApp*,

92 FACEBOOK finaliza aquisição do Whatsapp por US$ 22 bilhões. **Portal G1**. 2014. Disponível em: <http://tiny.cc/liui8y> Acesso em: 19 jun. 2019.

93 WELCH, Chris. Apple completes Shazam acquisition, will make app ad-free for everyone. **The verge**. 2018. Disponível em: <http://tiny.cc/un2i8y> Acesso em: 19 jun. 2019.

"[...] **podemos** utilizar *cookies* para lembrar de suas escolhas, como as preferências de idioma, e personalizar nossos Serviços para você" (grifo nosso)[94]. O mais adequado seria elencar restritivamente todos os casos em que os dados poderão ser utilizados.

Como forma de facilitar o entendimento dos termos de uso à população geral, o criador francês Hugo Roy lançou o site "Termos de Serviço, N*ão* Li"[95] em que há o resumo dos aspectos mais importantes, classificando os termos conforme as condições impostas, que vão de A (excelente) à F (péssimo). O criador desde logo afirma: "'Li e Concordo com os Termos' é a maior mentira na web. Nosso objetivo é consertar isto".[96]

Para os GAFA (*Google, Apple, Facebook, Amazon*) e os FANG (*Facebook*, *Amazon*, *Netflix, Google*) as notas e os principais avisos foram:

1. **Google:** *Classe C.*
– Sua identidade é usada em anúncios exibidos para outros usuários;
– Este serviço pode coletar, usar e compartilhar dados de localização;
– O serviço pode ler suas mensagens privadas;
– Este serviço rastreia você em outros sites;
– O Google pode coletar a impressão digital do seu dispositivo.
[...]
2. **Apple:** *Ainda sem classe.*
– Este serviço pode coletar, usar e compartilhar dados de localização;
– Termos podem ser alterados a qualquer momento, a seu critério, sem aviso prévio ao usuário;
– Termos podem ser alterados a qualquer momento, a seu critério, sem aviso prévio ao usuário;
+ Apple fornece um método de exclusão para publicidade direcionada da Apple;
+ Apple.com tem uma restrição de idade de 13 anos.
[...]

94 WHATSAPP. **Informação Legal do Whatsapp**. Disponível em: <https://www.whatsapp.com/legal/?lang=p t_br#privacy-shield> Acesso em: 19 jun. 2019.

95 Tradução livre de "*Terms of service; didn't read*".

96 Tradução livre: "'*I have read and agree to the Terms' is the biggest lie on the web. We aim to fix that*".

3. **Facebook:** *Ainda sem classe.*

– Sua identidade é usada em anúncios exibidos para outros usuários;

– O aplicativo necessário para este serviço requer permissões de dispositivo amplas;

– Este serviço rastreia você em outros sites;

– Este serviço pode licenciar o conteúdo do usuário para terceiras partes.

– O serviço pode usar pixels de rastreamento, web beacons, fingerprinting etc.

[...]

4. **Amazon:** *Ainda sem classe.*

– Termos podem ser alterados a qualquer momento, a seu critério, sem aviso prévio ao usuário;

– Este serviço rastreia você em outros sites;

– Os usuários devem revisitar os termos periodicamente, embora no caso de alterações materiais, o serviço notifique-os;

– Este serviço obriga os usuários à arbitragem obrigatória no caso de disputas;

– Este serviço pode licenciar o conteúdo do usuário para terceiras partes.

[...]

5. *Netflix: Ainda sem classe.*

– Termos podem ser alterados a qualquer momento, a seu critério, sem aviso prévio ao usuário;

– Netflix reserva o direito de divulgar informações pessoais, sem notificação;

– Este serviço obriga os usuários à arbitragem obrigatória no caso de disputas;

+ Os termos e as páginas da política de privacidade são bem organizados e formatados.

– Cookies são obrigatórios.[97]

No mesmo sentido, ressalta-se a pesquisa de Yannis Bakos *et al.* intitulada "Alguém lê as letras pequenas?"[98], em que, analisando os acessos aos *End User License Agreements* (EULAs), similar aos "Termos de Uso", verificou se tal leitura é ou não efetuada pelos usuários. Os pesquisadores rastrearam 48.154 visitantes mensais em 90 companhias *on-line* para estudar quantos dos compradores em potencial acessam o contrato que estão

97 Conteúdos pesquisados separadamente para cada empresa, traduzidos livremente e agrupados em citação deslocada. TERMS of service; didn't read. Disponível em: <https://tosdr.org/index.html?#> Acesso em: 19 jun. 2019.

98 Tradução livre de "*Does Anyone Read the Fine Print?*".

prestes a consentir. Em seus resultados:

> Os dados indicam que os EULAs foram acessados por apenas 63 das 131.729 visitas aos softwares varejistas (0,05% de todas essas visitas) e em 44 visitas a empresas freeware (0,15%). [...] Esses números já dizem bastante, mas outra consideração é se os compradores que acessam o EULA realmente o leem. **Para os usuários deste grupo, o tempo médio na página do EULA foi de 59,4 segundos e o tempo mediano foi de 34 segundos.** (Observe que estamos definindo o 'acesso' como uma visita do EULA de pelo menos um segundo, para fins de obter um número conservadoramente alto de acessos do EULA.) **Quarenta e seis por cento desses acessos eram menos de 30 segundos e 92% eram menos de 2 minutos** (grifos nossos).[99]

Assim, os autores concluem que o custo do tempo para acessar e compreender os contratos é mais limitador do que encontrar o contrato em si. [100] O estudo da monetização do tempo, chamado de custo de oportunidade, já era ressaltado pelo economista Gary Becker em um artigo de 1965: *A Theory of the Allocation of Time* – A Teoria da Alocação do Tempo. Por meio do desenvolvimento econômico, a jornada de trabalho tendeu a diminuir, causando uma realocação do período não trabalhado para outras atividades. A título de exemplo, o custo de assistir uma peça não é apenas o pago para a admissão, mas também o valor em que a plateia disponibiliza do seu próprio tempo para a dedicação àquela tarefa (BECKER,

99 Original: "*The data indicate that EULAs were accessed in only 63 of the 131,729 visits to software retailers (0.05% of all such visits) and in 44 visits to freeware companies (0.15%). [...] These figures are already telling, but another consideration is whether shoppers who access the EULA actually read it. For users in this group, the average time on the EULA page was 59.4 seconds and the median time was 34 seconds. (Note that we are defining "access" as a EULA visit of at least one second, for purposes of obtaining a conservatively high number of EULA accesses.) Forty-six percent of these accesses were less than 30 seconds, and 92% were less than 2 minutes*". BAKOS, Yannis; MAROTTA-WURGLER, Florencia; TROSSEN, David R. Does Anyone Read the Fine Print? Testing a Law and Economics Approach to Standard Form Contracts. **Ssrn Electronic Journal**, [s.l.]. p.1-45, 2009. p. 22. Elsevier BV. http://dx.doi.org/10.2139/ssrn.1443256. Disponível em: <https://pap ers.ssrn .com/s ol3/papers.cfm?abstract_id=1443256. Acesso em: 30 abr. 2019.

100 Idem, p. 2.

1965, p. 493). O mesmo se dá em relação ao custo da leitura dos "Termos e Condições de Uso".

Em um estudo realizado pela Universidade *Carnegie Mellon* com base em usuários americanos, descobriu-se que se todos lessem anualmente as políticas de cada site que visitam, a nação americana gastaria por volta de 54 bilhões de horas lendo políticas de privacidade. Em perspectiva, uma pessoa necessitaria de 244 horas por ano para ler as políticas, ou seja, seria exigido de cada um por volta de 40 minutos por dia.[101] Com isso, em suas estimativas, se todos os americanos se dedicassem a ler os "Termos de Privacidade" palavra por palavra, perderiam por volta de $781 bilhões de dólares do seu custo de oportunidade. Nestes casos, há uma conversão do consentimento à uma mera formalidade, em virtude do desnível de poderes entre os cidadãos e os grandes coletores de informações (RODOTÀ, 2008, p. 150).

É inviável se pensar que algum usuário tiraria quase duas horas das suas vinte e quatro horas diárias para ler um "Termo de Uso" que sequer existe possibilidade de adequação e personalização. Além disso, não bastaria a leitura, mas a sua real compreensão do que ali está disposto, o que dificilmente ocorre para a maioria das pessoas, já que os termos postos são complexos e de difícil entendimento.

Outro estudo interessante é o "'Eu Concordo com os Termos e Condições': (como) os usuários leem a privacidade políticas on-line? Um experimento de rastreamento ocular"[102] de Nili Steinfeld, da *Ariel University* em Israel. O estudo buscou analisar como a apresentação dos "Termos de Uso", se totalmente disposto antes do "Li e Aceito" ou se disponível por meio de *link*, favoreceria ou não sua a leitura, por meio de análise da trajetória ocular. De um total de 128 estudantes, a 64 destes foram apresentados os "Termos de Uso" em forma de *link*, em que o indivíduo deveria ativamente clicar para realizar a leitura. Destes, apenas 20,3% (treze participantes)

101 MCDONALD, A. M., CRANOR, L. F. The Cost of Reading Privacy Policies. I/S: A Journal of Law and Policy for the Information Society, v. 4, n. 3, 2008, 543-568. p. 563. Disponível em: <http://hdl.handle.net/1 811/72839>. Acesso em: 20 jun. 2019.

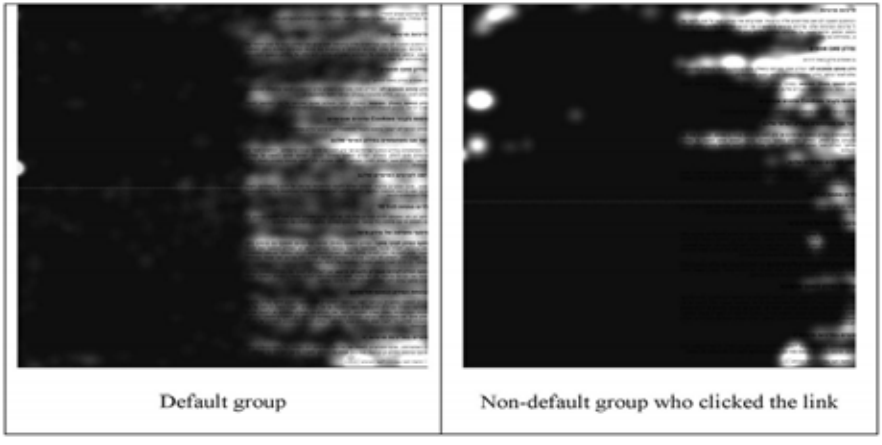
102 Tradução livre. "'*I agree to the terms and conditions': (How) do users read privacy policies online? An eye-tracking experiment*".

clicaram, enquanto 79,7% aceitaram os termos sem sequer abri-los.

Aos outros 64 estudantes, foram apresentados os "Termos de Uso" por padrão, ou seja, os temos apresentados integralmente antes do *checkbox* do "Li e Aceito". Destes, a média de tempo para a leitura do texto de 451 palavras foi de aproximadamente 1 minuto, o que indicou uma leitura minimamente dedicada.

Em figura abaixo sobre a análise da trajetória ocular, as partes transparentes são onde a visão foi direcionada por mais tempo. As laterais direitas estão mais claras pois a leitura foi realizada em hebraico, em que se lê da direita para a esquerda.

FIGURA 6 – FOCO OCULAR DOS DIVERSOS GRUPOS
Grupo padrão à esquerda e grupo que clicou no *link* à direita



Fonte: STEINFELD, Nili. 2016 "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. Computers In Human Behavior, [s.l.], v. 55, p. 992-1000, fev. 2016. Elsevier BV, p. 997. http://dx.doi.org/10.1016/j.chb.2015.09.038. Disponível em: <http://tiny.cc/r79raz>. Acesso em: 5 ago. 2019.

Os resultados destacam que, por meio do rastreamento ocular, ao contrário do que se poderia pensar, o grupo em que ativamente clicou no *link* para ler os "Termos de Uso", fez a leitura de forma menos interessada do que o grupo em que tais termos eram totalmente apresentados antes do *checkbox*. Portanto, segundo as análises do autor:

> Uma possível explicação para essa descoberta intrigante está no ato de clicar no link. É possível que ao clicar no link para ler a política, por si só, serviu como uma fonte de segurança para os usuários. **Ao realizar o clique, os participantes sentiram que haviam feito um esforço ativo para se tornarem informados e, ao fazê-lo, não mais sentiram a necessidade de realmente ler o documento.** O ato de clicar, que apenas um quinto dos participantes escolheu fazer, veio como compensação ao esforço de ler a política, e, por isso, **mesmo os poucos que saíram do seu caminho e clicaram para ler, apenas leram rápido o texto da política, em comparação com os participantes que foram apresentados a ela por padrão** (grifos nossos).[103]

Com isso, percebe-se que, a depender da arquitetura da informação e da disposição dos elementos pelos arquitetos virtuais, há a possibilidade de real de leitura pelos usuários, que não mais encerraria em um pseudoconsentimento. Essa divisão do consentimento em diversas partes é chamada de **granularidade do consentimento**, com a visão multifacetada da sua divisão em diversas concordâncias dos "Termos de Uso".

Diante disso, denota-se que as famosas cláusulas que encerram um rápido "Li e Aceito" pelo usuário, sem a devida facilitação da compreensão do conteúdo, são revestidas de um pseudoconsentimento não mais tolerado pela legislação. Até mesmo que se obtenha o consentimento em blocos, caso não seja possível a sua personalização pelo usuário, faz que os "Termos de Uso" e as "Políticas de Privacidade" não passem de um contrato de adesão consumerista.

103 Tradução livre: Original: "*One possible explanation for this puzzling finding lies in the act of clicking on the link. It is possible that clicking the link to read the policy, in itself, served as a source of reassurance for users. By clicking the link, participants felt that they had made an active effort to become informed, and having done so they no longer felt the need to actually read the document. The act of clicking the link, which only one-fifth of the participants chose to do, came at the expense of spending time and effort reading the policy, and so even the few who went out of their way and clicked to read the policy ultimately skimmed through the policy text, in comparison to participants who were presented with it by default*". STEINFELD, Nili. "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. **Computers In Human Behavior**, [s.l.], v. 55, p. 992-1000, fev. 2016. Elsevier BV. p. 998. http://dx.doi.org/10.1016/j.chb.2015.09.038. Disponível em: <http://tiny.cc/r79raz>. Acesso em: 5 ago. 2019.

2.4.6 As assimetrias inerentes aos "Termos de Uso": paradoxo da personalização

Os contratos digitais já tomaram robusta forma com o passar dos primeiros anos do século XXI. Esses contratos à distância, inicialmente chamados de contratos epistolares, já eram tratados pelo Código Civil de 1916 em seu art. 1.086.[104] Ainda antes, também foram tratados pelo Código Comercial de 1850 no art. 127, em que os contratos se reputam "concluídos e obrigatórios desde que o que recebe a proposição expede carta de resposta, aceitando o contrato proposto sem condição nem reserva".[105]

Os contratos digitais, portanto, passam a ser uma evolução de tais contratos epistolares, sendo capazes de formarem negócios jurídicos perfeitos. Em vez do instrumento "viajar" fisicamente até o destinatário, move-se eletronicamente em nanosegundos, revestindo-se, hoje, muitas vezes de "Termos de Uso (ou de Serviço)", que necessariamente citam e implicam "Políticas de Privacidade", "Políticas de *Cookies*", "Padrões da Comunidade", entre outros.[106] Além disso, em vez de ser a contratação entre ausentes por meio de correspondência em diferentes momentos temporais, é a contratação entre partes ausentes em tempo real (TUCCI, 2005).

Além das facilidades do contrato instantâneo, surge a personalização como o diferencial nas mais variadas tecnologias. Personaliza-se o tempo de sono necessário, consoante noites previamente analisadas por um

104 Art. 1.086. Os contratos por correspondência epistolar, ou telegráfica, tornam-se perfeitos desde que a aceitação é expedida, exceto: I – No caso do artigo antecedente. II – Se o proponente se houver comprometido a esperar resposta. III – Se ela não chegar no prazo convencionado.

105 Art. 127 – Os contratos tratados por correspondência epistolar reputam se concluídos e obrigatórios desde que o que recebe a proposição expede carta de resposta, aceitando o contrato proposto sem condição nem reserva; até este ponto é livre retratar a proposta; salvo se o que a fez se houver comprometido a esperar resposta, e a não dispor do objeto do contrato senão depois de rejeitada a sua proposição, ou até que decorra o prazo determinado. Se a aceitação for condicional, tornar-se-á obrigatória desde que o primeiro proponente avisar que se conforma com a condição.

106 Doravante serão citados apenas os Termos de Uso, por serem mais disseminados e por trazerem em seu bojo referência explícita aos demais modelos, mas as conclusões se aplicam a todos os outros indicados.

sistema, os filmes mais indicados baseados nos conteúdos já assistidos, a rota mais adequada ao trabalho... A tecnologia está apta a ser personalizada para melhoria de diversos aspectos da vida humana.[107]

A internet começou como uma internet de pessoas, conectando uns aos outros. Agora, com a internet das coisas, há a convergência da inteligência humana e a utilização das máquinas. A forma de operação dessas máquinas evolui cada vez mais, criando maneiras mais eficientes e adequadas às necessidades humanas. As coisas não apenas reagem a comandos, mas também socializam com outros dispositivos, tornando a informação, em si, inteligente.

Contraditoriamente, os contratos vinculados a tais tecnologias permitem nenhuma ou uma mínima personalização a cada usuário. Há mais um paradoxo: a personalização. Como afirma Gilberto Dupas ao tratar da ética na sociedade de informação, "O paradoxo está em toda parte" (DUPAS, 2001, p. 49).

Cada vez mais a publicidade é direcionada sem a necessária contrapartida sobre como ela é coletada. Para Shoshana Zuboff (2019, paginação irregular), essa personalização é mais uma das facetas do capitalismo de vigilância. O capitalismo informacional tomou para si uma nova lógica de acumulação, em que a coleta desenfreada de dados não tem uma contrapartida de proteção do indivíduo, tornando-o mera matéria-prima.

A autora, a exemplo de Castells que trata da sociedade informacional, indica o nascimento da civilização informacional. Contudo, indaga: será esta civilização um lugar que possamos chamar de lar em que se esteja a salvo do monitoramento? (IDEM, paginação irregular)

O compartilhamento das informações humanas por objetos, baseados em "Políticas de Privacidade e Termos de Uso", pouco indica se o indivíduo está realmente ciente deste constante monitoramento. Zuboff revela que essa mudança na civilização e a constante preocupação com o futuro da privacidade, revela o crepúsculo do ideário digital, tornando sua rápida mutação para o voraz capitalismo de vigilância. (IDEM, paginação irregular)

107 "Taylor aceitou os termos das políticas de privacidade da agência de viagens, da fornecedora dos aparelhos domésticos da sua casa, da companhia de táxi (ou da plataforma de 'caronas pagas'), do aeroporto, da companhia aérea, do seu relógio, da rede social, do hotel (ou da plataforma de 'acomodação'), do aplicativo de mensagens de treinos para corrida e, por fim, da sua seguradora de saúde." (BIONI, 2019. p. 24)

A ausência de personalização é característica marcante dos "Termos de Uso" atualmente e faz parte da sua definição. "Os Termos de Uso são contratos padronizados, definidos unilateralmente e oferecidos indiscriminadamente em igualdade de condições para qualquer usuário".[108] A sua unilateralidade já está no próprio vocábulo escolhido, que não deixa margem para a negociação: termos em vez de contratos, mas com pretensa executoriedade contratual.

No Brasil, a situação pode se delinear de forma favorável ao consumidor, ante existência de normas protetivas como o Código de Defesa do Consumidor, Lei n. 8.078 de 1990. Com isso, há uma mitigação da *pacta sunt servanda* e do princípio da autonomia da vontade, consoante estabelecido no art. 51[109] da norma, inserido na seção de cláusulas abusivas.

Em contrapartida, o tratamento de dados pessoais com a criação de

108 Tradução livre: "*Terms of Service are standardized contracts, defined unilaterally and offered indiscriminately on equal terms to any user*". VENTURINI, Jamila *et al.* **Terms of service and human rights:** an analysis of online platform contracts. Rio de Janeiro: Revan, 2016. p. 13. Disponível em: <http://bibliotecadigital.fgv.br/ds pace/handle/10438/18231>. Acesso em: 1º mai. 2019.

109 Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: I – impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis; II – subtraiam ao consumidor a opção de reembolso da quantia já paga, nos casos previstos neste código; III – transfiram responsabilidades a terceiros; IV – estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a eqüidade; V – (Vetado); VI – estabeleçam inversão do ônus da prova em prejuízo do consumidor; VII – determinem a utilização compulsória de arbitragem; VIII – imponham representante para concluir ou realizar outro negócio jurídico pelo consumidor; IX – deixem ao fornecedor a opção de concluir ou não o contrato, embora obrigando o consumidor; X – permitam ao fornecedor, direta ou indiretamente, variação do preço de maneira unilateral; XI – autorizem o fornecedor a cancelar o contrato unilateralmente, sem que igual direito seja conferido ao consumidor; XII – obriguem o consumidor a ressarcir os custos de cobrança de sua obrigação, sem que igual direito lhe seja conferido contra o fornecedor; XIII – autorizem o fornecedor a modificar unilateralmente o conteúdo ou a qualidade do contrato, após sua celebração; XIV – infrinjam ou possibilitem a violação de normas ambientais; XV – estejam em desacordo com o sistema de proteção ao consumidor; XVI – possibilitem a renúncia do direito de indenização por benfeitorias necessárias. [...]

perfis consumeristas pode levar a eventual discriminação do usuário por gênero, geolocalização, entre outros. Muitas vezes, essa discriminação não é sentida pelos indivíduos e, mesmo que percebida, o dano causado a uma pessoa, apesar de significativo no quadro geral, muitas vezes não é suficiente para a levar a discutir a questão extra ou judicialmente.

Para Danilo Doneda (2006, p. 377), a tentativa de transposição rasa do consentimento negocial ao consentimento do tratamento de dados pessoais não passaria de um "mito do consentimento". Apesar disso, a aplicação do Código de Defesa do Consumidor pode e deve ser alinhada com a LGPD, principalmente diante do excessivo tratamento pela nova legislação sobre forma de captação do consentimento.

Nos Estados Unidos, por exemplo, a matéria é tratada de forma diferente. A autora Shoshana Zuboff explica ao leitor americano que tais contratos são contratos de adesão, por impor condições *take-it-or-leave-it* para os usuários (ZUBOFF, 2019, paginação irregular). As cortes americanas, com relevância ao princípio da autonomia da vontade, determinam que tais contratos de adesão, por encerrarem em um "Li e aceito", são perfeitos e executáveis.

Apesar disso, até mesmo o *Chief Justice* da Suprema Corte dos Estados Unidos John Roberts já admitiu que não lê os termos de uso antes de aceitá-los. Segundo ele: "É um problema, porque o sistema legal obviamente é o culpado por isso".[110]

Mark Lemley explica que:

> A maioria das cortes, nos últimos dez anos, deu validade aos termos de uso, na teoria de que as pessoas concordam com os termos ao usar o software que já adquiriram. Por fim, e mais recentemente, um número crescente de cortes aplicou licenças 'browsewrap', nas quais o usuário não vê o contrato de forma alguma, mas em que os termos da licença determinam que o uso de um site constitui a aceitação de um contrato, o usuário estando ciente ou não.[111]

110 WEISS, Debra Cassens. Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print**. ABA Journal.** Disponível em: <http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the _computer_fine_pripr> Acesso em: 25 jun. 2019.

111 Tradução livre. "*A majority of courts in the last ten years have enforced shrinkwrap licenses,*

O autor esclarece que as licenças não significam um real consentimento do consumidor, tais como *shrinkwrap* (comum na década de 1980 e 1990, em que o termo é aceito pela compra e envio do produto, sendo os termos protegidos em invólucro de plástico),[112] *clickwrap* (quando os termos são aceitos com um breve clique) e *browsewrap* (o termo é aceito mesmo sem o usuário saber de sua existência, apenas pela navegação no site). Assim, no ambiente eletrônico de hoje, Mark Lemley defende que há a desintegração do consentimento (LEMLEY, 2006, p. 465).

O autor destaca ainda que a noção desses contratos imutáveis pressiona a noção clássica contratual:

> Os contratos de clique colocam alguma pressão sobre a noção clássica de consentimento derivada de acordos negociados, porque eles são substituídos por um consentimento geral *take-or-leave-it* para a noção clássica de que as partes realmente pensaram e concordaram com os termos do acordo.[113]

Assim, retoma-se o paradoxo da personalização, já que se aparenta que há pouco interesse em tornar executáveis meios de inserir a tecnologia de personalização também nas assinaturas de tais contratos.

Há as tentativas de formulação de *Privacy Enhancing Technologies* – PETs que se apresentem em ferramentas a serem aplicadas para a proteção dos seus dados pessoais. Entre elas se destacam a criptografia de mensagens trocadas, a anonimização dos dados pessoais, além de mecanismos de

---

on the theory that people agree to the terms by using the software they have already purchased. Finally, and more recently, an increasing number of courts have enforced 'browsewrap' licenses, in which the user does not see the contract at all but in which the license terms provide that using a Web site constitutes agreement to a contract whether the user knows it or not". (LEMLEY, 2006, p. 459-460)

112 LAMANCE, Ken. Shrink Wrap Agreement Lawyers. **Legal Match**. Disponível em: <https://www.legalmatch.com/law-library/article/shrink-wrap-agreements.html> Acesso em: 25 jun. 2019.

113 Tradução livre. "*Clickwraps put some pressure on the classical notion of assent derived from bargained agreements, because they substitute a blanket, takeit-or-leave-it assent for the classical notion that the parties actually thought about and agreed to the terms of the deal*". LEMLEY, Mark A. Terms of Use. **Minnesota Law Review**, Vol. 91, 2006. p. 466. Disponível em: https://ssrn.com/abstract=917926 Acesso em: 24 jun. 2019.

navegação anônima, entre outros (BIONI, 2019, p. 117).

Contudo, o problema dessas tecnologias não é propriamente a sua criação e seu desenvolvimento, mas sim a sua executoriedade. Aduz Bruno Bioni que a ferramenta *Do not track* – DNT – Não me rastreie – é uma PET que insere a autonomia do usuário na arquitetura dos sistemas de informação, em que com um breve clique no "DNT", estaria exteriorizada a escolha do usuário pela não coleta de dados. Contudo, não houve consenso sobre quem implementaria tal tecnologia, se a *World Wide Web Consortium* – W3C, organização de padronização da internet, ou se as entidades da indústria de publicidade comportamental. Além disso, ainda que alguns navegadores disponibilizem a funcionalidade, não há garantia de que realmente não haverá o rastreamento ante a ausência de executoriedade (IDEM, p. 179-181).

Há ainda a PET da *Platform for Privacy Preferences* – P3P – Plataforma para Preferência de Privacidade, que é um mecanismo em que o usuário poderia personalizar as suas preferências de privacidade e compartilhamento de dados para todos os sites que visitar em seu próprio navegador. Mais uma ferramenta de difícil execução, eis que para tanto, além dos navegadores adotarem tal funcionalidade, seria preciso que as aplicações tornassem suas políticas em formato legível para as diversas máquinas e não apenas para o usuário (IDEM, p. 182-183).

Bruno Bioni, em comentário sobre a P3P, mas que pode se aplicar à utilização das PETs aos Termos de Uso:

> [...] afastar-se-ia a lógica do 'tudo' ou 'nada' das políticas de privacidade, na medida em que o 'concordo' ou 'discordo' poderiam ser substituídos pela granularidade das autorizações especificadas nas preferências de privacidade. Assegurando-se tal poder de barganha na troca econômica (*trade-off*) da economia de dados, a P3P empoderaria o cidadão com uma autonomia genuína sobre o fluxo de suas informações pessoais. O leque de opções do processo de tomada de decisão avançaria para além da lógica binária do *take-it* ou *leave-it*. [grifos do autor] (IDEM, p. 184)

Inserido no contexto das PETs, como forma de *compliance* e adaptação

às novas regulações de dados pessoais, muitas empresas estão prevendo políticas de privacidade com base na *Privacy by Design* – PbD – ou privacidade desde a concepção. Para Bruno Bioni, a *Privacy by Design* "é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção de dados pessoais" (BIONI, 2019, p. 176).

Tal prática consiste em sete princípios,[114] mas foi estratificada para a prática em oito passos: a) Minimizar: a quantidade de dados pessoais processados deve ser mínima; b) Separar : o processamento de dados pessoais deve ser feito de forma distribuída sempre que possível, para evitar a criação de perfis para cada indivíduo; c) Agregar : dados pessoais devem ser processados no mais alto nível de agregação e com o menor detalhe possível em que eles são (ainda) úteis, de forma a preservar a identidade do titular; d) Esconder: quaisquer dados pessoais e suas interrelações devem ser de difícil acesso; e) Informar: os titulares dos dados devem ser adequadamente informados sempre que dados pessoais forem processados; f) Controlar : os titulares de dados devem ter a possibilidade de agenciar o processamento de seus dados pessoais; g) Executar: uma política de privacidade compatível com os requisitos legais deve estar em vigor e ser exequível e h) Demonstrar: instituir um controlador de dados para demonstrar conformidade com a política de privacidade e os requisitos legais aplicáveis (KOOPS et al., 2013).

Contudo, ante a ausência de personalização, a política da *Privacy by Design* não passa de contratos que expressam um "fique ciente do que eu faço e aceite da mesma maneira". Nigel Davies e Marc Langheinrich afirmam que a maior dificuldade na implementação das ferramentas de PbD pelos engenheiros de informática é a dificuldade de se quantificar a privacidade. "Você não administra o que você não quantifica" (DAVIES, LANGHEINRICH, 2013). Assim, apesar da boa premissa, a PbD, hoje, não

114 Princípios propostos por Ann Cavoukian em 1990: 1) Ser proativo e não reativo – Prevenir e não remediar; 2) Privacidade como configuração padrão; 3) Privacidade incorporada ao projeto; 4) Funcionalidade total – "Soma-positiva" em vez de invés de soma-zero; 5) Segurança de ponta a ponta – Proteção durante todo o ciclo de vida da informação; 6) Visibilidade e transparência; 7) Respeito pela privacidade do usuário – Solução centrada no usuário. (CAVOUKIAN, 2011)

atinge o nível de personalização necessário ao usuário.

Para Jamila Venturini *et al.*, esse problemático cenário de supostamente se concordar indistintamente com todos os "Termos de Uso" aos quais os usuários são expostos caracteriza uma falha de mercado, já que os consumidores em potencial não estão realmente considerando os termos contratuais para as suas tomadas de decisões. Assim, criam-se "Termos" com parâmetros antissociais e sem atingir as expectativas dos consumidores (VENTURINI, 2016, p. 14).

Na verdade, quem cala/clica para consentir, está buscando nada mais que a otimização do próprio tempo, já que: a) a depender do serviço, mesmo com suporte em português, a pessoa será obrigada a ler em língua estrangeira; b) ao final, não haverá qualquer adaptação e personalização dos "Termos".

A título de exemplo, na "Central de Privacidade e Segurança" da mídia social *Instagram*, o item "*Instagram Purchase Protection Policy*", na data da consulta, não está disponível em português.[115]

Destaca-se, além disso, o aplicativo de mensagens *WhatsApp*. Seus termos de uso constam um total de 20.450 palavras.[116] A velocidade média de leitura silenciosa dos brasileiros, partindo de dados de alunos da nona série de uma escola particular, é de 196,14 palavras por minuto.[117] Por simples regra de três, chega-se que ao dado que, para leitura integral para passar a utilizar a aplicação, o usuário comum gastaria, de forma arredondada, 104,26 minutos, ou seja, uma hora e quarenta e quatro minutos.

115 INSTAGRAM. **Central de Privacidade e Segurança**. Disponível em: <http://tiny.cc/o8387y>. Acesso em: 13 jun. 2019.

116 Dados obtidos pelo site: <https://www.whatsapp.com/legal/?lang=pt_br#key-updates>. Contagem realizada pela ferramenta de contar palavras, copiando o texto integral dos termos no Microsoft Word.

117 Dados fornecidos pela pesquisa "Velocidade de leitura e desempenho escolar na última série do ensino fundamental" de Eliana Komeno *et al.* KOMENO, Eliana Matiko *et al.* Velocidade de leitura e desempenho escolar na última série do ensino fundamental. **Estudos de Psicologia (campinas)**, [s.l.], v. 32, n. 3. p. 437-447, set. 2015. FapUNIFESP (SciELO). p. 441. http://dx.doi.org/10.1590/0103-166x2015000300009. Disponível em: <http://www.scielo.br/pdf/estpsi/v32n3/0103-166X-estpsi-32-03-00437.pdf>. Acesso em: 26 mar. 2019.

Destaque-se, ainda, que tal duração não é muito precisa[118], eis que tal brasileiro necessitaria conhecimento da língua inglesa, já que os tópicos "Pagamentos" e "*Privacy Shield*" dos Termos de Uso do *WhatsApp* não estão traduzidos.

O consentimento ainda é figura central para a utilização e tratamento de dados pessoais. Não se pode esperar, contudo, que nessa economia imediatista, em que o tempo e a velocidade em fechar contratos se transformaram, que se tenha o consentimento específico ou granular de todas as atitudes das empresas que receberam as informações. Ademais, demandar-se-ia um tempo absurdo da rotina dos brasileiros para poder empregar amplamente este consentimento.

Portanto, os atuais "Termos de Uso" não podem ser toleradas como totalmente vinculativos, eis que não partem de um efetivo consentimento do usuário. Não cabe aos consumidores uma real faculdade de leitura, tanto pela dificuldade de compreensão quanto por estarem em língua estrangeira. A utilização do clique "Li e Aceito" como forma nem tanto de obrigar os consumidores, mas sim de ocultar destes o fato de que seus dados serão utilizados para estratificação de perfis de consumo, torna-se, portanto, real prática abusiva.

118 A não ser que seja fluente, a velocidade de leitura por palavras por minuto de um brasileiro em inglês certamente diminuirá, sem se considerar, ainda, que grande parte da população não possui conhecimento de língua estrangeira.

3 Publicidade comportamental: táticas para a coleta de dados *on-line* e sua prejudicialidade

O que pensam os consumidores? A tentativa de desmistificar o consumidor é algo buscado pelas empresas de *marketing* há décadas, contudo, somente há pouco a análise das informações humanas por via digital se tornou possível.

Em pesquisa realizada por Roger Draper[119], na década de 1980, o cidadão americano estava exposto a 1.600 mensagens publicitárias por dia, percebendo ativamente 1.200 destas. Contudo, as pessoas apenas se interessavam ativamente por cerca de 12 delas, e tal resposta não era necessariamente positiva. Hoje, a capacidade de pe-

119 The Faithless Shepherd. **The New York Review Of** *Books*, Nova Iorque, 26 jun. 1986. Disponível em: <https://www.nybooks.com/articles/1986/06/26/the-faithless-shepherd/>. Acesso em: 4 nov. 2019.

netração da publicidade no cotidiano humano, mais precisamente no cotidiano do usuário da internet, revolucionou esta forma de comunicação.

Os rastros virtuais são capazes de identificar um ser humano em profundos níveis, algo que não é possível pela mera análise dos rastros físicos. Assim, em vez de uma corrida espacial, tem-se a corrida pela coleta de informações, destacando-se aquele que consegue coletá-la, analisá-la e estratificá-la para o seu retorno ao consumidor em forma de publicidade.

Ubiquitous computing, ou seja, a computação ubíqua/persuasiva será a expressão das próximas décadas. A indústria da atenção chegou ao feito de capturar o homem com um pequeno aparelho: o telefone celular. Deixando os cães para trás, o novo melhor amigo do homem é o *smartphone*, capaz de suprir as necessidades de comunicação, de carência e do que mais se possa imaginar. Tal amigo, contudo, não é bastante fiel. É um rastreador da atividade do seu companheiro; os algoritmos de seus aplicativos são constantemente alimentados com a inserção de dados e, verdadeiramente, tornam a maquininha capaz de entender o seu usuário.

Alan Westin (1967, p. 168-169) já afirmava que informação é poder, e que nunca a sociedade havia deixado tamanha pegada de dados pessoais. Certidões de nascimento e de casamento, históricos escolares, censos, registros militares, dados de passaporte, dados de coleta de impostos, contribuições de caridade, operações de cartões de créditos, entre muitos outros, há a geração de dados que, a depender de quem os controla, podem gerar uma vigilância indesejada.

As novas formas de registro, por sua vez, são bem-vindas para muitos ante os pretendidos benefícios da personalização. Todavia, "ninguém pode colher os benefícios da personalização se não estiver disposto a compartilhar as informações pessoais para que esses benefícios possam se tornar possíveis" (PEPPERS; ROGERS *in* KASANOFF, 2002, p. 14). Diferentemente, há alguns séculos atrás, a tentativa da realização de censos governamentais ensejou forte objeção do povo, que observava nesses registros um instrumento do Estado para a cobrança de impostos e alistamento militar (VIANNA, 2007, p. 89-90).

Inolvidável é, por exemplo, o banco de dados secreto produzido pelo Serviço Nacional de Inteligência (SNI), criado pela Lei n. 4.341, de 13 de junho de 1964, que contém dados de milhares de cidadãos e com

informações até hoje mantidas em sigilo (ZANON, 2013, p. 70).

A capacidade de compreensão das informações humanas pelas máquinas se releva, outrossim, pela constante exposição pessoal nas mídias sociais. Nas palavras de Andrew Keen (2012, p. 10), a mídia social é "aquela zona permanente de autoexposição de nossa nova era digital onde [...] publicamos coletivamente o retrato de grupo em movimento da humanidade". Continua, ainda, o autor a defender que tais mídias se tornaram não apenas uma segunda vida, em que se poderia ser o que quisesse, mas sim a própria vida, "o palco central e cada vez mais transparente da existência humana" (IDEM, p. 10). Portanto, o conceito de privacidade e de liberdade se confundem. O significado de liberdade talvez seja ninguém saber o que se está comprando ou com quem se está relacionando.[120]

Guy Debord teorizou, em 1967, a sociedade do espetáculo. Para o autor, "o espetáculo não é um conjunto de imagens, mas uma relação social entre pessoas mediada por imagens" (DEBORD, 1997, p. 14). Essas imagens, muitas vezes cercadas de publicidades de mercadorias, dominam a economia e encerram em um fetichismo da mercadoria. Gilberto Dupas (2001, p. 52), ao comentar o teórico francês, complementa que a degradação do "ser" para "ter" transformou-se no deslizamento do "ter" para o "parecer-ter".

Byung-Chul Han complementa a noção de mercadoria ao ampliá-la para a mercadoria humana:

> a "alegria" que se encontra nas redes sociais de relacionamento tem sobretudo a função de elevar o sentimento próprio narcísico. Ela forma uma massa de aplausos que dá atenção ao ego exposto ao modo de uma mercadoria".
> [...]
> Perdemos toda capacidade de admiração. Vivemos numa loja mercantil transparente, onde nós próprios, enquanto clientes transparentes, somos supervisionados e governados (HAN, 2018, p. 93, 128).

120 Conceito de Andrew Keen (2012, p. 12), em que defende que "Liberdade significava ninguém saber exatamente onde eu estava".

A supervisão se relaciona ao "Panóptico de Jeremy Bentham", cada vez mais referenciado e presente nas formas de interações virtuais. O utilitarista inglês, hoje, pode ser considerado o maior ícone da autoexposição. Em verdade, autoícone, posto que deixou consignado que doaria seu corpo para o *University College* de Londres, onde deveria ser exposto permanentemente em uma caixa de madeira com porta de vidro. Essa auto-exposição perpétua causou a reflexão de Andrew Keen (2012, p. 21):

> Eu vi a todos nós como Jeremy Bentham digitais, isolados uns dos outros, não apenas pela crescente ubiquidade das comunicações em rede, mas também pela natureza cada vez mais individualizada e competitiva da vida no século XXI. Sim, esse era o futuro. Reconheci que a visibilidade pessoal é o novo símbolo de status e poder em nossa era digital.[121]

E, assim, com a existência de uma extensa exposição dos usuários, é possível formular a figura do consumidor de vidro. Nesta conceituação ocorre a estruturação de bases de dados mais variadas, incluindo nelas o potencial decodificador das emoções dos usuários, tornando as emoções e características do consumidor totalmente transparentes (LACE, 2005, p. 1).

As dimensões das transparências das almas humanas notadas pelos estudiosos possuem o contraponto comum da hipermediação de entidades privadas na rede (VENTURINI, 2016, p. 12). A vida digital resta constantemente nas mãos privadas com a realização de mínimas ações diárias: o uso de internet mediante o pagamento a certo provedor; a utilização de buscadores como *Google* e *Yahoo*; o sistema operacional que se possui no computador etc. É dizer, a mediação dos entes privados na vida íntima dos indivíduos.

Estas companhias digitais, com óbvios fins lucrativos, regulam o acesso à internet por meio de "Termos de Uso" que se lê e aceita, divulgando

121 Vale mencionar o interessante projeto chamado *Panopticam Stream*, em que se instalou uma câmera acima da caixa de madeira de Bentham, pretendendo: "Observar você observando Jeremy Bentham". As fotos eram tiradas de hora em hora e publicadas no Twitter @PanoptiStream. Aparentemente, o projeto foi descontinuado em 2016, ante a ausência de atualização da conta na rede social.

informação de acordo com seus critérios e talvez a certo custo[122], coletando intermitentemente dados pessoais dos mais diversos agentes que se posicionem *on-line*.

Há, ainda, os hipermediadores, como *Amazon* e *Facebook*, que reúnem em si uma tremenda capacidade de absorção de informação pela multiplicidade de papéis que podem assumir, seja como rede social ou *market place*, vendedor ou intermediador. Todas as informações coletadas de todos os lados são utilizadas. A *Amazon*, por exemplo, ao mesmo tempo que possibilita que vendedores avulsos se utilizem de seu *market place,* vende e produz os mesmos produtos, tendo a vantagem competitiva de saber todas as informações pessoais dos consumidores e de lucros de seus competidores, que, paradoxalmente, estão incluídos na mesma plataforma (KHAN, 2016, v. 126, p. 710-805).

Assim, as possibilidades das novas tecnologias "vão além daquilo que o homem jamais teve possibilidade de administrar anteriormente" (DONEDA, 2006, p. 37). Nos novos modelos de negócios digitais a publicidade útil e direcionada se faz essencial para o aumento do consumo de produtos e de serviços.

Tornou-se necessário captar as ânsias de uma geração e convertê-las em verdadeiros objetos de desejo. As informações pessoais, assim, tornaram-se altamente relevantes para personalização da experiência. Essa personalização, contudo, resta maculada quando realizada por práticas ocultas de rastreamento do usuário. Elas violam frontalmente os fundamentos estabelecidos sobre a disciplina da proteção dos dados pessoais no Brasil, tais como o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, da honra e da imagem.

Nas demonstrações de cultura popular, como filmes e séries, o amor de Theodore pela assistente virtual, Samantha, como mostrado

122 Em 2019, a rede social Instagram implementou testes no Brasil e no Canadá para a ocultação no número de *likes* da plataforma. O usuário poderia ver a quantidade de suas fotos, mas não de fotos alheias. A decisão buscaria uma plataforma mais real e que valorizasse o conteúdo em vez de números. Contudo, muitas críticas surgiram, pois, em tese, a ocultação dos *likes* serviria para a rede de forma que os criadores de conteúdo tivessem que pagar a ferramenta de publicidade para que suas publicações alcançassem seus seguidores.

no filme *Her*, não mais parece uma realidade distante e inalcançável. Ainda no ramo televisivo, destaca-se a série *Westworld*, que trata de um parque de diversões em que adultos interagem com robôs, onde as máquinas captam as reações humanas para fins ocultos de análises mercadológicas e publicitárias; acertada a afirmação de Robert Ford, criador do parque: "Cada pedaço de informação no mundo foi copiado e feito backup, exceto a **mente humana – o último dispositivo analógico em um mundo digital**"[123] (grifos nossos). Segundo Shoshana Zuboff, com a reorientação do poder da informação, não mais se pretende que esta penas flua sobre os indivíduos, mas que haja uma automação humana (ZUBOFF, 2019, cap. 1, paginação irregular).

Partindo desses pressupostos, no primeiro subtópico objetiva-se descobrir interesses de particulares na propaganda informatizada, destacando a dimensão do *big data* para o comércio eletrônico, bem como a sua revolução para a nova forma publicitária. No segundo subtópico, ainda de forma a analisar como se dá a modelagem comportamental com o direcionamento de publicidade, estudam-se os métodos *data mining, profiling e big data analytics,* que se destacam como forma de coletar, de estratificar e de correlacionar, respectivamente, as informações dos consumidores na rede.

Partindo disto, na subseção 3.2.1, destacam-se as principais práticas ocultas de direcionamento mais comuns, tais como *cookies*, *web beacons*, *supercookies,* HTML *5 Web Storage* e *fingerprinting*, demonstrando a sua evolução de forma a tornar o rastreio quase imperceptível, bem como para analisar a clareza com que demonstram ao usuário da coleta e da estratificação de seus dados. Por fim, no último subtópico enumeram-se alguns casos marcantes das correlações prejudiciais do *big data analytics* com potencial prejuízo aos usuários/consumidores/cidadãos.

Vale ressaltar que não se pretende demonizar as tecnologias de direcionamento de publicidade como um todo. Consoante Gilberto Dupas (2001, p. 18):

123 Tradução livre. "*Every piece of information in the world has been copied and backed up, except the human mind – the last analog device in a digital world*". WESTWORLD. Produção de Jonathan Nolan e Lisa Joy. Los Angeles: Home Box Office – HBO, 2018, Les Écorchés, S02E07, 15:44-15:56.

> Não se trata de ir contra o desenvolvimento tecnológico, adotando um posicionamento reacionário. A questão é bem outra: a tecnologia pode e deve se submeter a uma ética que seja libertadora a fim de contemplar o bem-estar de toda a sociedade, presente e futura, e não apenas colocar-se a serviço de minorias ou atender necessidades imediatas.

Assim, busca-se uma análise crítica para buscar a função social da tecnologia na sociedade do século XXI.

3.1 A dimensão do *big data* para o comércio eletrônico

O *big data é de difícil* conceituação, já que ele está em constante evolução. Em 2013, menos de 2% da informação arquivada no mundo era não-digital; hoje, o percentual deve estar ainda menor (CUKIER; MAYER-SCHOENBERGER, 2013, v. 92, p. 1). O termo, apesar de frequentemente citado no cotidiano, não exige uma definição perfeita para a sua compreensão, podendo ser definido como um **volume**[124] de dados monumental, processado em enorme **velocidade**, com uma indispensável **variedade** de dados para a riqueza informacional, implicando nesta variedade a **veracidade** das informações, para que os dados possam perfeitamente aderir à realidade.

A partir da pretensa definição, tem-se os famosos "Vs" do *big data*. Doug Laney (2001, p. 1-4), partindo da observação do *big data* principalmente no âmbito do comércio eletrônico, analisou a gestão de dados pelas empresas de tecnologia e apresentou os primeiros três destes "Vs": volume, velocidade e variedade. A partir de então, o acréscimo de "Vs" ao termo é feito por variados autores de acordo com seus critérios de definição do fenômeno.[125] No entanto, o volume é o mais indispensável

124 De acordo com Kenneth Cukier e Viktor Mayer-Schoenberger (2013, p. 1) se toda a informação contida no *big data* fosse inserida em CDs e, sendo estes empilhados, formar-se-iam cinco pilhas separadas em que todas alcançariam a lua.

125 Cf. MCNULTY, Eileen. Understanding big data: the seven V's. **Dataconomy**, 22 maio 2014. Disponível em: <http://dataconomy.com/2014/05/seven-vs-big-data/>. Acesso em: 18 set. 2019. RIJMENAM, Mark van. Why the 3 V's are not sufficient to describe big

para a definição. Para Ripon Patgiri e Arif Ahmed (2016, p. 17), há muitos "Vs" no paradigma do *big data*, todavia "Todos os Vs do Big Data – Volume ≠ Big Data".

É importante ter em mente, contudo, que o big data não é um sistema inteligente. Como afirma Bruno Bioni, não se trata de uma forma de inteligência artificial, mas sim de uma inovadora metodologia de estruturação de dados e a partir dessa estruturação é feito o cálculo da probabilidade de ocorrência de certo evento. O *big data* "não está preocupado com a análise das razões que geram uma cadeia de eventos, mas, tão somente, com o seu desencadeamento" (BIONI, 2019, p. 41-42).

Além de metodologia, para Cukier e Mayer-Schönberger, o *big data* é caracterizado como a habilidade de "renderizar" dados em quantidades jamais vistas – a chamada "datatificação". Consoante os autores:

> Em vez de tentar "ensinar" a um computador como fazer as coisas, como dirigir ou traduzir línguas distintas, o que especialistas em inteligência artificial têm tentado sem sucesso por décadas, **a nova abordagem é alimentar dados o suficiente em um computador de forma que ele possa inferir da probabilidade** de que, digamos, um semáforo seja verde e não vermelho ou que, em um determinado contexto, *lumière* seja um substituto mais apropriado para "luz" do que para leger (grifos nossos) (CUKIER; MAYER-SCHOENBERGER, 2013, v. 92, p. 1).

Tais probabilidades tiradas da inovadora metodologia *big data*, tornam-se cada vez mais acuradas. Quanto mais se alimentam os dados, melhor material os algoritmos possuem para trabalhar, dando às correlações maior poder de conexão, em todos os sentidos, retroalimentando, assim, a sua potência tecnológica.

Um exemplo disto é a ferramenta de busca do *Google*, serviço de buscas que se aperfeiçoa com base nas próprias buscas do usuário. Atualmente, dificilmente encontra-se usuário que utilize a internet em

data. **Datafloq**, ago. 2015. Disponível em: <https://datafloq.com/rea d/3vs-sufficient--describe-big-data/166>. Acesso em: 18 set. 2019.

uma base minimamente regular que utilize outra plataforma de busca. De uma forma ou de outra, os resultados fornecidos pelo *Google são mais certeiros ante o volume de buscas que o próprio efetua. Ou seja, o alto volume d*e dados inseridos favorece a variedade e o alcance da informação buscada e, consequentemente, devolvida ao usuário em forma de *links*.[126] Assim, a concorrência de outros buscadores com a exatidão dos resultados do *Google* resta comprometida, já que quanto menos pesquisas são realizadas, pior o seu algoritmo de estratificação de dados.

Consoante Viktor Mayer-Schönberger e Kenneth Cukier:

> Muitas empresas projetam seus sistemas para que eles possam coletar dados exaustivamente e reciclá-los, para melhorar um serviço existente ou para desenvolver novos. O Google é o líder indiscutível. Ele aplica o princípio de 'aprender com os dados' a muitos de seus serviços.[127]

As plataformas digitais, entre elas as redes sociais, atuam cada vez mais como a definição de mercado de dois lados, em que dois grupos distintos se unem por meio de uma estável plataforma (fisicamente e/ou

126 Cientistas americanos foram capazes de rastrear a ocorrência de gripes epidêmicas por meio de registros arquivados de pesquisas no Google, em que usuários pesquisavam os sintomas no buscador. Os dados se relacionaram a um real aumento de casos de gripes nas áreas pesquisadas. "*Google web search queries can be used to estimate ILI [Influenza-Like Illness] percentages accurately in each of the nine public health regions of the United States. Because search queries can be processed quickly, the resulting ILI estimates were consistently 1-2 weeks ahead of CDC [Centers for Disease Control and Prevention] ILI surveillance reports.* ***The early detection provided by this approach may become an important line of defence against future influenza epidemics in the United States, and perhaps eventually in international settings***" (grifos nossos). GINSBERG, Jeremy; MOHEBBI, Matthew; PATEL, Rajan *et al.* Detecting influenza epidemics using search engine query data. **Nature**, v. 457, n. 7232. p. 1012-1014, 2009. Disponível em: <https://www-nature.ez11.periodicos.cap es.gov.br/articles/nature07634>. Acesso em: 18 set. 2019.

127 Tradução livre: "*Many companies design their systems so that they can harvest data exhaust and recycle it, to improve an existing service or to develop new ones. Google is the undisputed leader. It applies the principle of recursively 'learning from the data' to many of its services*". CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. **Big Data:** A Revolution That Will Transform How We Live, Work, and Think. E-book. Boston: Houghton Mifflin Harcourt, 2013. paginação irregular.

financeiramente), que age a conectar grupos que, sem esta, dificilmente poderiam se conectar.[128]

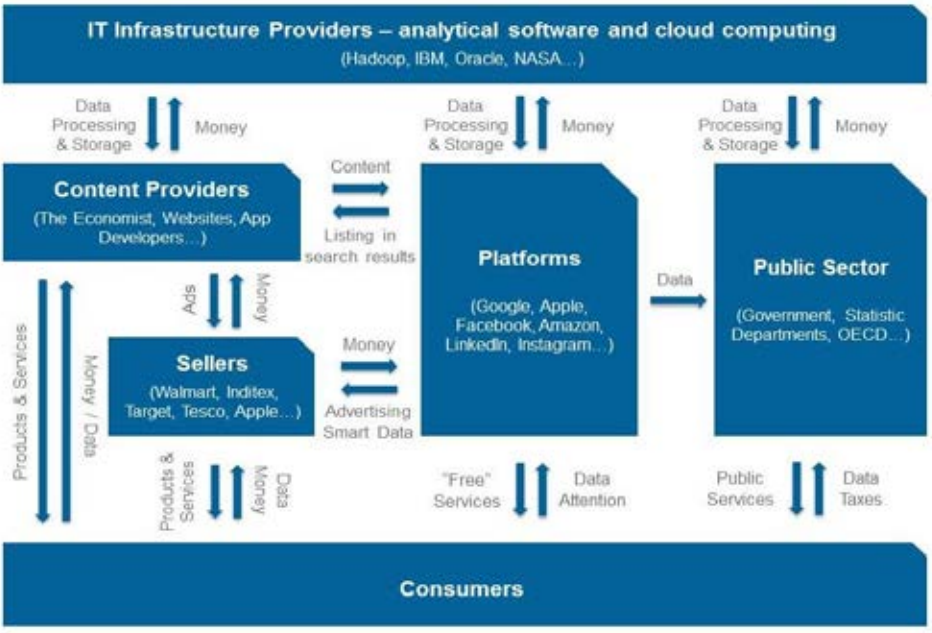
Os *shoppings centers são um* clássico exemplo de mercado de dois lados. As plataformas já existiam; o disruptivo das plataformas digitais é a própria internet. Estas, por sua vez, agem de forma multilateral, cortejando múltiplos lados em seus negócios. Isto é possível graças a interação com o *big data*.

Na nota "*Big Data*: Trazendo as Políticas Concorrenciais para a Era Digital", da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), o órgão analisa o ecossistema do *big data* como sendo: "coletado, transacionado e convertido em valor monetário em um complexo ecossistema composto de múltiplos mercados interconectados, muitos dos quais são multilaterais".[129] Elucida, ainda, a multilateralidade por meio da figura a seguir:

128 A primeira proposta de definição do mercado de dois lados (M2L) foi realizada por Rochet e Tirole: "*Two-sided (or more generally multi-sided) markets are roughly defined as markets in which one or several platforms enable interactions between end-users, and try to get the two (or multiple) sides 'on board' by appropriately charging each side. That is, platforms court each side while attempting to make, or at least not lose, money overall*". ROCHET, Jean-Charles; TIROLE, Jean. Defining Two Sided Markets. **IDEI**, Toulouse. p.1-28, 2004. p. 1. Disponível em: <http://tiny.cc/z52ycz>. Acesso em: 18 set. 2019.

129 Tradução livre: "*Big Data is collected, transacted and converted to money value in a complex ecosystem composed of multiple interconnected markets, many of which are multi-sided*". ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. **Big Data**: Bringing Competition Policy to the Digital Era. Paris. DAF/COMP (2016)14, 40 p. 2016. p. 12. Disponível em: <http://tiny.cc/yg4ycz>. Acesso em: 18 set. 2019.

FIGURA 7 – ECOSSISTEMA DO BIG DATA



Fonte: ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. **Big Data: Bringing Competition Policy to the Digital Era**. Paris. DAF/COMP (2016)14, 40 p, 2016, p. 12. Disponível em: <http://tiny.cc/yg4ycz>. Acesso em: 18 set. 2019.

As plataformas são agentes conectores de toda a economia. As suas interconectividades e hiperconectividades geram novas soluções e, possivelmente, novos problemas. Deste modo, é interessante a análise da figura acima, pois nela se constata que a indústria da atenção possui inegável papel na coleta de dados, que ao oferecer seus "serviços gratuitos", indiretamente fornece dados próprios para o marketing das empresas que anunciam, ou não, em sua plataforma. Assim, consoante o relatório supracitado, os consumidores remuneram a plataforma com a sua atenção e, portanto, suas buscas orgânicas[130] são intercaladas com publicidade. De modo similar, eles são obrigados a assistir a um anúncio antes de obter acesso a um conteúdo.[131]

130 Aquilo que o usuário realmente busca na utilização da plataforma.

131 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE.

A economia de atenção organiza os rastros culturais dos usuários. Portanto, como aduz Ramus Helles e Mikkel Flyverbom: "Nos espaços digitais, nossas ações e vidas são traduzidas em recursos que podem ser usados para alimentar processos comerciais, culturais, e políticos e para guiar nossos olhos e atenção".[132]

Com isto, gera-se a ilusão de gratuidade das maiores plataformas e mídias de atenção. O seu modelo de negócio é propriamente a captação de dados pessoais e, como não pedem remuneração direta ao usuário, são pagas pelos anunciantes para realizar a publicidade direcionada.

Como explica Bruno Bioni, atualmente há a figura do *prosumer*, em que o consumidor passa a atuar ativamente, deixando de ser um espectador no ciclo de consumo. "O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer.*" (grifos do autor) (BIONI, 2019, p. 15).

A proatividade do consumidor que busca se inserir na rede, tanto para aquisições no comércio on-line como para buscar avaliações e avaliar produtos, enriquece a rede do *big data*, consequentemente aumentando seu volume e sua variedade para uma melhor probabilidade de uma futura personalização.

Não obstante, é necessário questionar-se quem possui amplo poder de detenção e estratificação dessas informações em primeira mão.

*É inegável que o m*undo digital permite, cada vez mais, a concentração do poder econômico. Por exemplo, no depoimento de Mark Zuckerberg ao Senado dos Estados Unidos, por ocasião do vazamento de dados da *Cambridge Analytica*, ao ser questionado pelo senador Lindsey Graham, que lhe perguntou: "Quem é o seu maior concorrente?", o criador do

Big Data: Bringing Competition Policy to the Digital Era. Paris. DAF/COMP(2016)14, 40 p, 2016. p. 12. Disponível em: <http://tiny.cc/yg4ycz>. Acesso em: 18 set. 2019.

132 Tradução livre: "*In digital spaces, our actions and lives are translated into resources that may be used to fuel commercial, cultural, and political processes and to guide our eyes and attention*". HELLES, Rasmus; FLYVERBOM, Mikkel. Meshes of Surveillance, Prediction, and Infrastructure: On the Cultural and Commercial Consequences of Digital Platforms. **Surveillance Society**, [s.l.], v. 17, n. 1/2. p.34-39, 31 mar. 2019. Queen's University Library. p. 34. Disponível em: <http://dx.doi.org/10.24908/ss.v17i1/2.13120>. Acesso em: 24 set. 2019.

Facebook enfrentou certas dificuldades em nomear algum competidor direto. Em resposta genérica, disse: "Senador, nós temos muitos concorrentes [...]. Você quer apenas um? Não tenho certeza se posso dar um, mas posso dar vários?".[133] As empresas indicadas, contudo, *Google*, *Apple*, *Amazon* e *Microsoft*, não são exatamente concorrentes diretas do total que o *Facebook* e os aplicativos de seu grupo, *Instagram* e *WhatsApp*, representam.

Ainda no referido relatório da OCDE, trata-se do possível monopólio das plataformas digitais multilaterais:

> As características multilaterais das plataformas tendem a levar, como resultado de uma rede de externalidades diretas e indiretas, **à concentração de usuários e seus respectivos dados nas mãos de poucos jogadores.** Por sua vez, o uso do *Big Data* fornece às plataformas on-line um poder de mercado substancial no fornecimento de serviços essenciais de informação, nos quais todas as empresas e os consumidores confiam. [...] Alta lucratividade *per se* não implica danos competitivos, desde que o sucesso dos negócios seja alcançado por meio de inovação baseada em dados e **não pela exploração do B*ig* D*ata* para discriminar alguns jogadores, para impor custos de troca, para garantir contratos exclusivos ou para executar outras formas de abuso** (grifos nossos).[134]

133 Para transcrição desta parte do depoimento, Cf.: JEONG, Sarah. Zuckerberg struggles to name a single Facebook competitor. *The Verge*. Washington. 10 abr. 2018. Disponível em: <https://www.thever ge.com/2018/4/10/17220934/facebook-monopoly-competitor--mark-zuckerberg-senate-hearing-lindsey-graham>. Acesso em: 19 set. 2019.

134 Tradução livre: "*The multisided features of platforms tend to lead, as a result of direct and indirect network externalities, to the concentration of users and their respective data in the hands of a few players. In turn, the use of Big Data provides online platforms with substantial market power in the supply of essential information services, upon which all companies and consumers rely. […] High profitability per se does not imply competitive harm, as long as business success is achieved through means of data-driven innovation, and not through exploitation of Big Data to discriminate against some players, impose switching costs, enforce exclusive contracts, or conduct other forms of abuse*". ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. **Big Data:** Bringing Competition Policy to the Digital Era. Paris. DAF/COMP(2016)14, 40 p, 2016. p. 13. Disponível em: <http://tiny.cc/yg4ycz>. Acesso em: 18 set. 2019.

Consoante se vê na Figura 2[135], as maiores empresas da atualidade são de tecnologia. Nesse ambiente concentrado de *big techs*, os riscos de monopólio e manipulação indevida de dados são inerentes. O desafio da defesa do consumidor em um ambiente significativamente concentrado envolve não somente a aplicação de deveres da legislação consumerista, mas também a defesa da livre concorrência e a proteção de privacidade e dos dados pessoais.

Contextualmente, o *Facebook já foi multado*, em 2017, pela Comissão Europeia em €110 milhões, por fornecer informações conflituosas sobre sua fusão com o *WhatsApp*, com base no artigo 14 da *Merger Regulation* (Regulação do Conselho n. 139/2004).

Diferentemente do compromisso firmado perante a Comissão em 2014, em 2016 o *Facebook* incluiu *melhoria* nos produtos do *WhatsApp*, em que indicava o compartilhamento informações dos usuários entre as ambas plataformas. Com isso, a Comissão Europeia considerou que a empresa forneceu informações enganosas em seu compromisso de forma, no mínimo, negligente.[136]

Também em 2017, o *Facebook* foi multado pela Agência Espanhola de Proteção de Dados (AEPD) em €1,2 milhões por coletar, armazenar e utilizar informações para fins publicitários sem prévia autorização. Ainda, a multa se deu por base na ausência de esclarecimento aos usuários que haveria *cookies* da empresa os rastreando em sites que não são do *Facebook*, mas que contém o botão curtir.[137]

O *Bundeskartellamt* – órgão de antitruste alemão – recentemente decidiu pela restrição da coleta de dados pelo Facebook aos seus usuários. Além disso, a empresa não pode mais unificar os dados obtidos em outras plataformas, como *Instagram* e *WhatsApp*, com os dados do *Facebook* para direcionamento de anúncios, a não ser que para isso obtenha específico

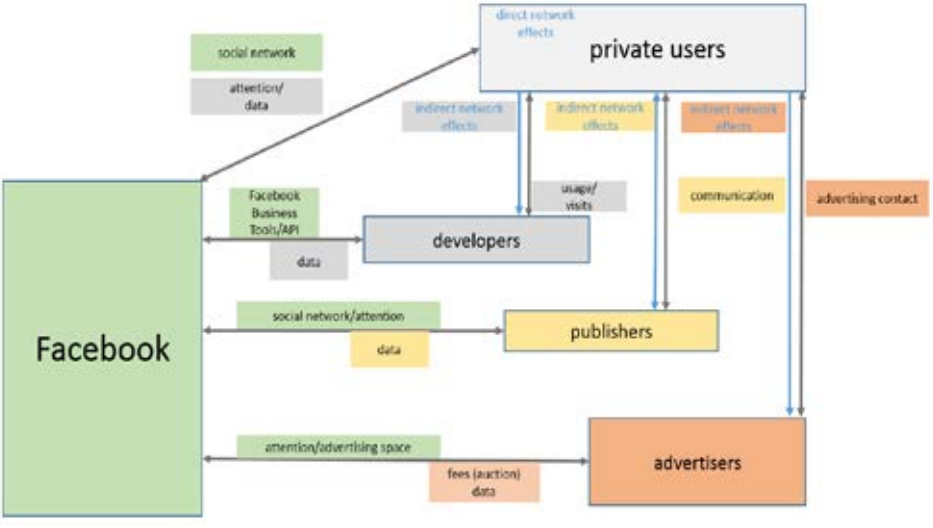
135 Capítulo 2, subitem 2.1.

136 COMISSÃO EUROPEIA. **Case M.8228 – Facebook/Whatsapp**. 17 maio 2017. Disponível em: <https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf> Acesso em: 20 set. 2019.

137 AGÊNCIA ESPANHOLA DE PROTEÇÃO DE DADOS – AEPD. **Resolución: R/01870/2017**. 11 set. 2017. Disponível em: <https://www.aepd.es/resoluciones/PS-00082-2017_REC.pdf> Acesso em: 05 out. 2019.

consentimento. Para a autoridade, o *Facebook* adquire com esse compartilhamento um poder de mercado e uma dominância que torna impossível que qualquer concorrente possa competir. Tal decisão abrange tanto uma dimensão econômica, mais precisamente concorrencial, como uma dimensão dos direitos fundamentais dos usuários de internet. Segundo gráfico da própria autoridade, assim é o funcionamento do modelo de negócio do *Facebook*:

FIGURA 8 – MULTILATERALIDADE DO FACEBOOK



Fonte: BUNDESKARTELLAMT. **Administrative Proceedings Decision under Section 32(1) German Competition Act** *(GWB) B6-22/16*. Bonn, 06 fev. 2019, p. 64. Disponível em: <http://tiny.cc/xnu3cz>. Acesso em: 20 set. 2019.

Após aproximadamente três anos do que se poderia chamar de um processo administrativo, foi proferida decisão que pode servir de paradigma para análises de casos futuros envolvendo outras empresas de tratamento de dados para direcionamentos publicitários. Houve ordem de implementação das mudanças necessárias para adaptar a sua política de dados e *cookies* em um período de doze meses. Em agosto de 2019, o *Facebook* obteve vitória perante o Tribunal de Segunda Instância

Oberlandesgericht Düsseldorf[138], deferindo suspensividade em relação a decisão do *Bundeskartellamt*. Após recursos, a análise sobre a legalidade da decisão do órgão será proferida pelo tribunal superior *Bundesgerichtshof*, que é o equivalente ao Superior Tribunal de Justiça no Brasil.

Diferentemente do caso anterior do *Facebook* analisado pela Comissão Europeia, não houve imposição de multas, mas a declaração que parte da "Política de Privacidade" da empresa é ilegal e não se coaduna com o GDPR, nem com a legislação alemã de defesa da concorrência. Ademais, a decisão atesta que o *Facebook*, em comparação com seus pretensos concorrentes *Google +, Stayfriends*, *StudiVZ*, *Jappy* e *Wize.Life*[139] – partindo da análise do número de usuários diários – apresenta poder de mercado quase monopolístico de 95% dos usuários.[140]

A dimensão e estruturação do *big data*, portanto, aparenta dar maior poderio àqueles que sabem usufruir dessa superestrutura de dados. Para Shoshana Zuboff, a dificuldade de se definir o *big data* surge do erro em persistir em vê-lo como um efeito tecnológico. Ele surge no social, a partir da lógica intencional e consequencial do capitalismo e vigilância. Sendo o combustível dessa nova forma de capitalismo, o *big data* busca prever e modificar o comportamento humano como meio de produzir lucros e controle de mercado.[141] Em sua obra sobre o capitalismo de vigilância, afirma que:

138 VI-Kart 1/19 (V).

139 Houve a diferenciação entre redes sociais e mídias sociais, como o Youtube, não sendo este, portanto, levado em comparação. Foram desconsiderados Twitter e Snapchat por fornecerem apenas parte dos serviços oferecidos pelo Facebook, não podendo serem incluídos no mercado relevante. Além disso, não se considerou o LinkedIn, por ser uma rede social de objetivo especificamente profissional.

140 Para a autoridade: "'*Daily active users' are users who use the network at least once a day. With an increasing user-based market share, Facebook's share of the market affected comes close to a monopolistic position. In the period under review no competitor has thus been able to achieve a user-based market share higher than 5%*". BUNDESKARTELLAMT. **Administrative Proceedings Decision under Section 32(1) German Competition Act (GWB) B6-22/16**. Bonn, 06 fev. 2019. p. 110. Disponível em: <http://tiny.cc/xnu3cz>. Acesso em: 20 set. 2019.

141 ZUBOFF, Shoshana. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal of Information Technology**, [s.l.], v. 30, n. 1. p.75-89, mar. 201. p. 75. SAGE Publications. Disponível em: < http://dx.doi.org/10.1057/jit.2015.5>. Acesso em: 14 mar. 2019.

> A conexão digital é agora um meio para fins comerciais de outros. Na sua essência, o capitalismo de vigilância é parasitário e autorreferencial. Ele revive a antiga imagem de Karl Marx do capitalismo como um vampiro que se nutre de trabalho, mas com uma reviravolta inesperada. Em vez de trabalho, o capitalismo de vigilância se alimenta de todos os aspectos da experiência de todo ser humano.[142]

A autora ainda atesta que, nos primeiros anos da *World Wide Web*, houve uma preocupação pelo *Google* sobre a eventualidade de se cobrar para ter acessos ao seu então recente sistemas de buscas. Como solução da questão, eles optaram, em vez, pelo modelo de anunciantes. "Eventualmente restou claro que o negócio do Google é o leilão de palavras-chaves, e seus clientes são os anunciantes".[143] Pode-se complementar, ainda, que os usuários do sistema de buscas são a matéria-prima para o aperfeiçoamento algorítmico.

Essa abordagem de aquisição dos dados do usuário como material para funcionamento dos próprios algoritmos para vender e direcionar propagandas foi, como se percebe até hoje, um grande sucesso. A partir do modelo de sucesso do *Google*, a ciência do *big data*, como chama a autora, disseminou-se.[144]

Como se vê, muito além de dados, o *big data* é, principalmente, sobre pessoas. Essa lógica de acumulação adquire caráter sensível quando se percebe que *não se está apenas acumulando dados*, mas também características pessoais de usuários da internet. A análise fria de um dado não é com-

142 Tradução livre: "*Digital connection is now a means to others' commercial ends. At its core, surveillance capitalism is parasitic and self-referential. It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of labor, surveillance capitalism feeds on every aspect of every human's experience*". (ZUBOFF, 2019, cap. 1, paginação irregular)

143 Tradução livre: "*Eventually it became clear that Google's business is the auction business, and its customers are advertisers*". ZUBOFF, Shoshana. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. **Journal Of Information Technology**, [s.l.], v. 30, n. 1. p.75-89, mar. 201. p. 79. SAGE Publications. Disponível em: <http://dx.doi.org/10.1057/jit.2015.5>. Acesso em: 14 mar. 2019.

144 Idem, p. 79.

patível com o dever de proteção de direitos humanos e de personalidade.

Este contexto de *big data* inclui a *Web* 3.0,[145] em que, além dos seres humanos, as máquinas possuem inegável papel em alimentar o conteúdo da internet. Os algoritmos, por exemplo, são passos lógicos para a execução de determinada tarefa automatizada. A probabilidade que se infere do *big data* é a pura correlação entre os dados e as estatísticas as quais se busca encontrar.

Segundo Kenneth Cukier e Viktor Mayer-Schönberger, o apelo pela confiança nas ferramentas de análise de dados é tentador, contudo, a análise "dataísta" deixa de lado um elemento eminentemente humano: a imprevisibilidade. Os instintos, as tomadas de riscos e a capacidade de errar são características que ainda não são adaptadas às máquinas. Para os autores, "Haverá uma necessidade especial de criar um lugar para o humano: reservar espaço para intuição, bom senso e acaso para garantir que não sejam lotados de dados e respostas feitas por máquinas" (CUKIER; MAYER-SCHOENBERGER, 2013, p. 7).[146]

Infelizmente, muito sobre a capacidade de captação de dados das empresas e a sobreposição destes dados em perfis pessoais ainda não são de ciência ou preocupação do usuário-consumidor, apesar da emergência de diversas leis e regulamentos de proteção de dados pessoais.

Como exemplo, expõe-se uma experiência realizada pelo *InternetLab* em um vídeo chamado "E quando te pedem informações pessoais em uma compra?".[147] Em um caixa de farmácia, no momento do pagamento, o atendente iniciou uma série de perguntas e pedidos

145 Eduardo (Magrani, ao explicar o conceito: "O termo Web 3.0 foi criado pelo jornalista John Markoff, do New York Times, baseado na evolução do termo Web 2.0 difundido por Tim O'Reilly e Dale Dougherty em 2004. Enquanto a Web 2.0 permitia a interação entre pessoas, a Web 3.0 usará a Internet para cruzar dados. Essas informações poderão ser lidas pelos dispositivos e estes conseguirão fornecer informações mais precisas". (MAGRANI, 2019, p. 48)

146 Tradução livre: "[…] *there will be a special need to carve out a place for the human: to reserve space for intuition, common sense, and serendipity to ensure that they are not crowded out by data and machine-made answers".* (CUKIER; MAYER-SCHOENBERGER, 2013, p. 7)

147 INTERNETLAB. **E quando te pedem informações pessoais em uma compra?**. You Tube. Disponível em: <https://www.youtube.com/watch?v=uHZs3ADb6RQ> Acesso em: 25 set. 2019.

para conclusão da compra. A maioria das pessoas ofereceu normalmente o CPF, prática já cotidiana para muitos brasileiros. Em seguida, solicitou-se uma foto para o cadastro. Apesar da desconfiança, sem maiores explicações os consumidores autorizaram a foto. Solicitou-se, ainda, uma foto de perfil. De forma ainda mais invasiva, pediu-se o cadastramento das impressões digitais de vários dedos, ato, repise-se, autorizado por diversas pessoas no vídeo. Ressalte-se que tudo isto com a promessa de descontos e promoções.

De forma ainda mais curiosa, as perguntas continuaram: "Qual seu melhor amigo?", "Você tem animal de estimação?" ou "Qual o nome da sua mãe?". Apesar da ausência de correlação destas perguntas e das coletas dos dados pessoais e biométricos com a compra a ser efetuada, as pessoas continuavam respondendo.

Se diante de um espectador humano fazendo as perguntas, considerando que as pessoas ficam mais retraídas em compartilhar seus dados, houve uma abertura considerável para sua vida pessoal, imagine-se quando a coleta é realizada de forma automatizada por um consentimento concedido de forma acrítica em algum "Termos de Uso e Política de Privacidade".

Podem-se encarar como preocupantes as tendências universalizantes do *big data*. Em seu protótipo de influir probabilidades a certos eventos a partir de seu imenso volume de dados, resta indagar sobre o perfil das pessoas que alimentaram essa rede. É importante ressaltar que milhares de pessoas ainda vivem na periferia tecnológica do mundo. O acesso à rede ainda resta inatingível para diversas populações do globo, que sequer possuem suas necessidades básicas e fisiológicas atendidas.

Consoante Jonas Lerman, o *big data* é grande ferramenta no processo decisório público e privado. Contudo, tende-se a olvidar que nesse incontável volume de dados está inerente a possibilidade de erros, geralmente desconsiderada em relação à grandeza dos números obtidos. No entanto, a maior parte dos dados em si é produzida por pessoas totalmente inseridas na vida digital. Ou seja, alguém que recebe o pagamento em dinheiro, não usa cartão de crédito, não se inscreve em programas de desconto e não usa aplicativos de transporte simplesmente também não se insere no *big data*, o que transforma estes dados em um espelho apenas daqueles

que o alimentam.[148]

Afirma o autor que em um futuro que o *big data* e suas previsões são inerentes à vida social, ele reordenará fundamentalmente o governo e o mercado, realizando uma progressiva exclusão das pessoas pobres e marginalizadas dos conjuntos de dados. Isto terá implicações preocupantes nas oportunidades econômicas, na mobilidade social e na participação democrática.[149] A famosa expressão "*We are Big Data*" possui sentido até indagar-se sobre quem está incluído neste "n*ós*".

É nesse contexto social que acontecem abusos de diversas magnitudes. Com o ordenamento de tais informações obtidas, podem ocorrer excessos, não unicamente relacionados ao preço de um produto, mas também abusos que se revestem em custos de oportunidade e em perdas de chances de vida.

3.2 *Big Data* e publicidade: a modelagem comportamental por meio do *profiling* e do *machine learning*

A internet é, acima de tudo, uma criação cultural (CASTELLS, 2003, p. 32). Assim, reflete, de início, as próprias implicações e modelos econômicos da sociedade que a criou. Após as últimas décadas de intensa penetração social, a internet passa, enfim, a ditar os novos comportamentos sociais e a possuir grande influência no cotidiano dos cidadãos. Vigendo o sistema capitalista também em domínio digital, as questões de publicidade estão diretamente a ele ligadas.

A propaganda, frequentemente confundida com o *marketing*, ***é um dos pilares deste e se relaciona diretamente ao sentido de promoção,*** sendo para Aida Lovison "qualquer forma de comunicação em caráter não pessoal paga por um patrocinador identificado sobre um bem tangível, intangível

148 LERMAN, Jonas. Big Data and Its Exclusions. **Ssrn Electronic Journal**, [s.l.]. p.55-63, 2013. p. 59. Elsevier BV. Disponível em: <http://dx.doi.org/10.2139/ssrn.2293765>. Acesso em: 20 set. 2019.

149 Idem, p. 59.

ou para campanhas de mudança de comportamentos e ideias".[150] A publicidade seria outro pilar do marketing, tomando um aspecto mais amplo que a propaganda.

Na visão do filósofo utilitarista Jeremy Bentham, a publicidade é um princípio fundamental da política democrática,[151] mesmo que este não se refira, em um primeiro plano, à publicidade de consumo.

Em tendo o mundo digital cada vez mais relevância para a vida social, é inegável a transformação publicitária para acompanhar a dinamicidade social na internet. Como aduz Cristiane Carvalho, "Toda e qualquer transformação na vida das pessoas, na economia social, nas dinâmicas culturais, implica em mudanças da prática publicitária".[152]

O economista francês Serge Latouche, ao criticar o sistema capitalista que busca um crescimento sem objetivos, aduz que a sociedade capitalista se utiliza de uma ronda diabólica da publicidade, relacionando esta ao desejo; ao crédito, que fornece os meios; e *à* obsolescência dos produtos para que eles sejam constantemente necessários. "A publicidade nos faz desejar o que não temos e desprezar aquilo que já desfrutamos" (LATOUCHE, 2009, P. 17-18).

A abordagem presumidamente diabólica da publicidade se relaciona principalmente à publicidade predatória e oportunista. Para John Berger (1999, p. 144):

> O objetivo da publicidade é tornar o espectador ***l*geiramente insatisfeito com seu atual modo de vida.** Não com o modo de vida da sociedade, mas com o seu próprio, enquanto nela

150 LOVISON, Aida Maria; PETROLL, Martin de La Martinière. Ética na publicidade e propaganda: a visão do executivo de agências de comunicação do Rio Grande do Sul. **Cadernos Ebape.br**, [s.l.], v. 9, n. 2, p.333-359, jun. 2011. FapUNIFESP (SciELO). Disponível em: <http://dx.doi.org/10.1590/S1679-39512011000200007>. Acesso em: 25 set. 2019.

151 BENTHAM, Jeremy. Da publicidade. **Revista Brasileira de Ciência Política**, [s.l.], n. 6. p.277-294, dez. 2011. FapUNIFESP (SciELO). Disponível em: <http://dx.doi.org/10.1590/S0103-33522011000200011>. Acesso em: 25 set. 2019.

152 CARVALHO, Cristiane Mafacioli. Gênero, linguagem e estratégias do discurso publicitário da atualidade. **Revista Famecos**, [s.l.], v. 19, n. 3. p.821-838, 2 jan. 2013. EDIPUCRS. p. 822. Disponível em: <http://dx.doi.org/10.15448/1980-3729.2012.3.12903>. Acesso em: 25 set. 2019.

> inserido. A publicidade sugere que se ele comprar o que ela está oferecendo, sua vida se tornará melhor. **Oferece-lhe uma alternativa melhorada do que ele é.** (grifos nossos)

Para Everardo Rocha (1990, p. 25), a publicidade revelada aos consumidores é vista como mágica: "Lá, no mundo do anúncio, a criança é sempre sorriso, a mulher desejo, o homem plenitude, a velhice beatificação. Sempre a mesa farta, a sagrada família, a sedução. Mundo nem enganoso nem verdadeiro, simplesmente porque seu registro é o da mágica".

Muitas vezes, a publicidade foi apontada como negativa, bem como as atividades a ela relacionadas, como aponta André D'angelo (2003, v.7, n.4, p. 55-75), remontando a Platão e Aristóteles, à Bíblia, a Confúcio e *à* literatura grega clássica. O autor defende, ainda, que a vertente do *marketing* em que os fins justificam os meios deve ser superada, "merecendo ser substituída por uma vertente deontológica, em que os *meios* utilizados para atingimento dos *fins* ***são tão importantes quanto estes***" (IDEM, p. 64). (grifos do autor)

Portanto, a utilização da publicidade em si não é uma prática a ser combatida, já que por diversos anos ela foi um meio de reafirmar o sistema capitalista em vigor. Resta, contudo, debater os limites éticos para a realização da publicidade, principalmente em matéria de acesso a um grande contingenciamento de dados, como é hoje a figura do *big data*.

Ante a perda de eficácia da comunicação em massa como era realizada desde o último século, a descoberta da possibilidade de direcionamento em massa de anúncios, revestiu o ramo de um poder de influência no ser humano sem precedentes.

Para Bruno Bioni (2019, p. 16), a publicidade direcionada foi concebida a partir da concepção que a própria comunicação em massa era ineficiente. Os esforços em focar no público alvo desde o início da atividade publicitária é relevante para a diminuição de custos de dissipação dos anúncios entre pessoas que manifestamente não faziam o seu perfil alvo.

Mencionado autor passa então a dissecar a **publicidade direcionada** em seus três aspectos: a publicidade **contextual** (aspecto objetivo), **segmentada** (aspecto subjetivo) e **comportamental**, sendo a última o objeto da presente pesquisa. A publicidade **contextual** é aquela que encontra

seu público pela sua inserção em determinado ambiente, on-line ou off--line. O que a classifica é o meio onde é promovido o anúncio, como propagandas de vendas de veículos em revistas automobilísticas ou anúncios de livros com temática política em cadernos de política em jornais (BIONI, 2019, p. 16).

A publicidade **segmentada**, enquanto aspecto subjetivo, supera o contexto físico ou virtual em que o anúncio será veiculado para focar no público que será alcançado. O alcance de público é menor, mas mais específico, pois os anúncios são direcionados ao público independentemente do contexto da plataforma (IDEM, p. 17). Diferentemente da anterior, em que o público atingido seria apenas aqueles leitores de revistas ou jornais, a publicidade segmentada se adapta à hipótese dos anúncios no *Facebook* ou *Instagram* que, partindo das características do usuário, direcionam certo anúncio a adolescentes ou jovens adultos, por exemplo.

Por fim, chega-se à publicidade **comportamental** *on-line* em que, partindo da coleta de dados da atividade do usuário, como os *cookies*, pode--se inferir seus interesses e mostrar anúncios com mais relevância (IDEM, p. 19). Esse grau de personalização é inédito na história publicitária, continuando o autor que:

> Por isso, a publicidade comportamental *on-line* reduz os custos da ação publicitária, uma vez que o bem de consumo anunciado é correlacionado cirurgicamente aos interesses do consumidor abordado. A comunicação com o público-alvo daquele produto ou serviço é praticamente certeira, *ocasionando maior probabilidade de êxito quanto à indução ao consumo* (grifos nossos) (IDEM, p. 19).

A publicidade da internet pode ser potencialmente destrutiva, pois jamais se teve acesso ao caráter íntimo do consumidor, principalmente quando se age amparadas em práticas ocultas e abusivas, tornando difícil ao usuário comum a descoberta de uma indução comportamental.

No arcabouço jurídico brasileiro, o Decreto Federal n. 2.181/1997, que dispõe sobre o Sistema Nacional de Defesa do Consumidor, em seu art. 19, condena a publicidade abusiva e enganosa com multa, ficando sujei-

tos ainda aqueles que veicularem "publicidade de forma que o consumidor não possa, fácil e imediatamente, identificá-la como tal".

O Código Brasileiro de Autorregulamentação Publicitária do Conselho Nacional de Autorregulamentação Publicitária (CONAR), apesar de não se ocupar expressamente da propaganda subliminar, em seu art. 29 condena "quaisquer tentativas destinadas a produzir efeitos 'subliminares' em publicidade ou propaganda". Ademais, qualquer veiculação de publicidade mediante pagamento deve ser propriamente identificada para evitar a confusão do consumidor.

As regulações acima, contudo, não parecem suprimir adequadamente a ocorrência da publicidade comportamental, ou sequer a encaram como realidade na sociedade de informação.

A indagação "O que pensam os consumidores?" deixou de ser uma questão existencial aos profissionais da área, já que, com a facilitação do *big data*, a partir das ferramentas de *machine learning*, as máquinas passaram a criar perfis – *profiling* – sobre os consumidores.

A questão se expande ante a autoexposição do usuário nas mais diversas redes sociais. A partir desta, o ser humano se torna verdadeira matéria prima para a personalização dos anúncios. Essa personalização muitas vezes passa despercebida pelos usuários, mas não é incomum se pensar que, por vezes, o dispositivo leu a mente do usuário ou ter um determinado anúncio de produto que o persegue na rede.

Para Byung-Chul Han, a exposição da intimidade nas mídias sociais é realizada de forma acrítica:

> Hoje em dia, as coisas só começam a ter valor quando são vistas e expostas, quando chamam atenção. Hoje, nos expomos no Facebook, e com isso nos transformamos em mercadoria. [...]. O hipercapitalismo transforma todas as relações humanas em relações comerciais. Ele arranca a dignidade do ser humano, substituindo-a completamente pelo valor de mercado (HAN, 2018, p. 125-127).

Em contrapartida, para Nicolas Carr, os seres humanos não são somente criaturas sociais, mas criaturas privadas. "O que não partilhamos é

tão importante quanto o que partilhamos".[153] É o mesmo que dizer que a música é feita a partir de seus silêncios.

Com o surgimento das redes sociais, a solidão de muitos foi abrandada com a conexão intermitente, valorizando-se, por exemplo, atualizar continuamente os amigos sobre a própria localização. Contudo, esse ar de *hobby* que permeia tais redes poderá ser facilmente dissipado a partir da percepção que há um rastreamento intermitente para fins publicitários.

Tim Wu, em seu livro "*The Attention Merchants*" traz a premissa que a atenção é a nova *commodity* do século XXI:

> Desde a ascensão do capitalismo, sabe-se que capturar a atenção de alguém pode render algum dinheiro. [...] Com a publicidade, [ela] foi o mecanismo de conversão que, com surpreendente eficiência, transformou a safra de atenção em *commodity* industrial. Dessa forma, a atenção poderia não apenas ser usada como revendida, e é aqui que nossa história começa. [154]

Essa *commodity* adquire outra dimensão quando relacionada às ferramentas de anúncio como as do *Facebook* e do *Google*. Em vez de uma pretensa gratuidade da utilização do serviço, por não haver uma contraprestação pecuniária direta, encontram-se os serviços[155] em que a cessão de

153 Tradução livre: "*What we don't share is as important as what we do share*". CARR, Nicholas. Tracking Is an Assault on Liberty, With Real Dangers. **The Wall Street Journal**. Disponível em: <https://www.wsj.com/articles/SB10001424052748703748904575411682714389888> Acesso em: 25 set. 2019.

154 Tradução livre: "*Since the rise of capitalism, it has been known that capturing someone's attention could cause him to part with some money. [...] For advertising was the conversion engine that, with astonishing efficiency, turned the cash crop of attention into an industrial commodity. As such, attention could be not only used but resold, and this is where our story begins*". WU, Tim. **The attention merchants**: the epic scramble to get inside our heads. Nova Iorque: Alfred A. Knopf, 2016. p. 20-21.

155 Para Bruno Bioni, há ainda os serviços *fremium*, em que a partir da combinação do gratuito (free) com serviços pagos (*premium*), atrai-se o consumidor à utilização ferramentas gratuitas para, após, instigar o consumidor a adquirir a versão completa por meio do *premium*. Como exemplo destes negócios estão a maioria dos *streamings* de música, aplicativos de anotações, armazenamentos em nuvem etc. No entanto, o autor ressalta que mesmo em pacotes *premium*, os serviços continuam a monetizar os dados do usuário da mesma forma que no serviço gratuito, à exemplo do Dropbox. (BIONI, 2019, p. 27).

dados pessoais possibilita a existência destes negócios pretensamente gratuitos. Como aduz Bruno Bioni, "[s]ão os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico" (BIONI, 2019, p. 25). Por isso, não é incomum que seja negado acesso a sites por pessoas que usam funções de bloqueador de anúncios.

A possibilidade de aprendizado por meio de dados na internet, portanto, aumenta exponencialmente de rapidez da percepção do público sobre determinada campanha. Enquanto nas antigas propagandas de televisão a demora para obter a reação do público era inerente, o *feedback* do sucesso de uma campanha ou anúncio na internet ***é obtido em segundos.***

A partir desse aprendizado por meio de dados é que se obtém o *machine learning* que, segundo Cathy O'Neil, o computador se emerge em dados, seguindo básicas instruções até que o algoritmo nele relacionado encontra padrões próprios e, com o tempo, conecta-os com certos resultados, de certo modo, obtendo um aprendizado (O'NEIL, 2016, p. 67).

Partindo do exemplo da autora, cientistas tentaram ensinar, desde 1960, computadores a ler partindo de programações em que inseriam códigos de definições e de regras gramaticais. No entanto, as ***língua***s são formadas principalmente por gírias e exceções, tornando quase impossível que a máquina leia com base apenas em regras codificadas. Com a massiva utilização da internet nos últimos anos, possibilitou-se que, a partir de uma imensidade de dados, o aprendizado se desse de forma mais rápida e eficiente. A ferramenta *Siri*, da *Apple*, bem como a *Alexa*, da *Amazon*, são exemplos do massivo aprimoramento do *machine learning* (IDEM, p. 68).

A partir desse método de aprendizagem das máquinas, busca-se estabelecer correlações. Tal correlação pode implicar na criação de perfis comportamentais e estes perfis, com base em dados passados, fazem análises futuras, a exemplo de uma bola de cristal, com o diferencial de possuírem grande precisão.

A criação de perfis comportamentais é chamada de *profiling*, em que há uma captação, análise e segmentação da informação, sendo capaz de criar o perfil pessoal de alguém e potencialmente aplicá-lo em forma de estereótipo. Na definição de Bruno Bioni, o *profiling* é a prática em que "os dados

pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet" (BIONI, 2019, p. 91).

Laura Schertel Mendes define a construção de perfis como uma reunião massiva de dados do indivíduo, "com a finalidade de se obter uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de padrões de comportamento, de gostos, hábitos de consumo e preferências do consumidor" (MENDES, 2014, p. 111).

Este conglomerado de técnicas é o *big data analytics*. A análise do *big data* pode ser realizada de diversas formas, contudo, o risco de utilização antiética é uma constante neste território digital, em que é difícil ter controle e regulação eficazes.

Consoante os estudos de Dennis Hirsch, as companhias de cartões de crédito, ao tentar encontrar futuros clientes que fossem bons pagadores, buscaram uma simples correlação em seu enorme bancos de dados.

Curiosamente, a correlação mais precisa foi a de que pessoas que compravam almofadas antidesgaste de pisos possuíam consideravelmente menos dívidas com cartões de crédito. Como aduz o autor,

> A análise não explicou por que isto ocorreu. Poderia ter sido que aqueles que cuidam de seus pisos mostram a mesma responsabilidade em relação às suas contas de cartão de crédito. Ou, pode ter sido que aqueles que possuem finos pisos de madeira geralmente mobiliam almofadas antidesgaste e que esses indivíduos são mais ricos ou têm um caráter diferente do que a população geral. Ou, poderia ter sido algo completamente diferente (grifos nossos).[156]

Apesar de existirem correlações altamente benéficas à sociedade hiperconectada, como a correlação de tratamentos médicos que funcionam melhor

156 Tradução livre: "*The analysis did not explain why this was so. It could have been that those who take care of their floors show the same responsibility with respect to their credit card bills. Or, it could have been that it is those who have nice, wooden floors that generally furniture anti--scuff pads, and that these individuals are wealthier or have a different character than the general population. Or, it could have been something else entirely*". HIRSCH, Dennis. Predictive Analytics Law and Policy: A New Field Emerges. *I/s: A Journal Of Law And Policy For The Information Society*, Ohio, v. 14, n. 1. p.1-9, 2017. p. 3. Disponível em: <http://hdl.handle.net/1811/86703>. Acesso em: 24 set. 2019.

a certos pacientes ou de identificação de transações potencialmente fraudulentas em bancos,[157] também possuem inferências inerentemente negativas.

Dennis Hirsch define os quatro principais riscos da utilização indiscriminada e impensada do *big data analytics*: risco à privacidade, risco de viés, risco ao erro e risco de exploração.

Para o risco à **privacidade,** enquanto um site de vendas utiliza correlações para indicar produtos; nestas mesmas correlações podem obter-se dados sobre a sexualidade, orientação política, situação financeira etc.[158] Ou seja, são correlações que implicam diretamente na autonomia humana de se revelar seletivamente ao mundo.

Quanto ao risco de **viés**, poder-se-ia determinar quem teria direito a certas oportunidades de vida. Assim, com a potencial exclusão daqueles que permanecem na periferia dos dados do *big data*, um sistema que é alimentado e metodologicamente utilizado a partir dos dados de quem os alimentam, tende a se perpetuar um sistema excludente.

Por exemplo, a correlação para se identificar quem potencialmente pretende ficar grávida a curto prazo pode influir diretamente na contratação de uma mulher a certo posto. Ou até mesmo, criar correlações entre raças e religiões para identificar qual raça ou religião seria melhor pagadora, de forma a negar aos pretensamente identificados como maus pagadores oportunidades financeiras.[159] Até mesmo a correlação de um perfil de consumo para direcionar os preços de acordo com a capacidade econômica (BIONI, 2019, p. 90).

A base do *big data analytics*, ou seja, a correlação, primeiro aponta resultados para depois os humanos construírem razões. Funciona como uma pesquisa científica ao avesso, em que primeiro se têm ocorrências confirmadas, para após estabelecerem-se as hipóteses que as obtém.

Para Cathy O'Neil, ao tratar dessa análise em seu livro *Weapons of Math*

157 HIRSCH, Dennis. Predictive Analytics Law and Policy: A New Field Emerges. *I/s: A Journal Of Law And Policy For The Information Society*, Ohio, v. 14, n. 1. p.1-9, 2017. p. 4. Disponível em: <http://hdl.handle.ne t/1811/86703>. Acesso em: 24 set. 2019..

158 Idem, p. 4.

159 Idem, p. 5.

Destruction: [160]

> Um componente essencial desse sofrimento é o pernicioso *loop* de *feedback*. Como vimos, os modelos que perfilam uma pessoa por suas circunstâncias ajudam a criar o ambiente que justifica as suas premissas. Este ciclo destrutivo gira e gira, e no processo, o modelo se torna cada vez mais injusto.[161]

Outro exemplo de Dennis Hirsch sobre o ciclo de discriminação a partir dos algoritmos é a análise que a probabilidade de um candidato homem de suceder a altos cargos é maior do que essa probabilidade na contratação de uma candidata mulher. Contudo, as correlações já estão viciadas, já que, ao perpetuamente contratar homens para altas posições, pois estas confirmam seu sucesso, perpetua o ciclo tóxico de desigualdade (HIRSCH, 2017, v. 14, n. 1, p. 6). Ou seja, a partir de dados falhos, tem-se atitudes discriminatórias, mesmo que não diretamente intencionadas pelo desenvolvedor.

Ainda, pesquisadores da Universidade Federal de Minas Gerais, baseando-se nas perguntas sobre se é possível identificar estereótipos na beleza feminina na internet, bem como se raça e idade influenciam nessas pesquisas, apresentaram resultados relevantes sobre o aprendizado algorítmico a partir de preconceitos humanos.

Ao pesquisar os termos "mulher feia" e "mulher bonita" no *Google* e no *Bing* em diversos países, partindo das 50 primeiras imagens que apareciam nas pesquisas, formou-se um banco de dados que foi submetido a uma análise facial. Entre os principais estereótipos, estavam para os negativos mulheres velhas e negras, bem como para os positivos mulheres brancas e jovens, repetindo-se estes em quase todos os continentes (ARAÚJO; MEIRA; ALMEIDA, 2016, p. 419-437).

160 Há um trocadilho entre *mass* e *math*. Geralmente utiliza-se a expressão correlativa em inglês "armas de destruição em massa". A autora, por sua vez, trocou massa (*mass*) por *math* (matemática), implicando que os cálculos algorítmicos são armas de destruição.

161 Tradução livre: "*A key component of this suffering is the pernicious feedback loop. As we've seen, sentencing models that profile a person by his or her circumstances help to create the environment that justifies their assumptions. This destructive loop goes round and round, and in the process the model becomes more and more unfair*". (O'NEIL, 2016, p. 30)

Apesar de não serem apontadas as razões para tais estereótipos, como um exemplo de uma pretensa falta de diversidade em bancos de fotos, há grande possibilidade de eles derivarem de um discriminatório *machine learning* que, a partir das fotos mais clicáveis pelos usuários, identifica-se um padrão de beleza estereotipado.

Isso infere diretamente no risco ao **erro**, em que algoritmos falhos perpetuam predições falhas. Isto é tratado pela Margaret Hu em "*Big Data Blacklisting*" – para a autora, é o processo de categorização administrativa de indivíduos como "culpados até que se provem inocentes" (HU, 2016, p. 1735).

Inolvidável o conto de fadas Alice no País das Maravilhas em que, no momento do julgamento da Alice, as palavras da Rainha foram: "Primeiro a sentença, o veredito depois". Enquanto o veredito seria a determinação se era culpada ou inocente, a sentença, que seria a pena, foi primeiramente proferida: "Cortem-lhe a cabeça!" (CARROLL, 2015, p. 134). O uso da informação para criar um perfil pessoal, além de cercear um possível direito de defesa, torna os prejuízos de decisões semiautomatizadas quase impossíveis de serem remediadas.

A inclusão de pessoas no *Terrorist Watchlist* ou no *No-fly list*, como ocorre nos Estados Unidos, principalmente após os ataques de 11 de setembro de 2001, é particularmente sensível, pois possivelmente[162] muitos desses dados foram associados não somente partindo de dados públicos, mas também de dados coletados em ramos privados que focam na captura e correlação de dados (HU, 2016, p. 1788).

As questões de segurança nacional se tornam excessivamente sensíveis quando se pretende criar um perfil do cidadão, não possuindo este direito a questionar tal perfil já que, muitas vezes, sequer sabe que é discriminado por isto. Consoante André Dias Fernandes, ao tratar da Lei n. 9.614/98 (Lei do Abate):

> Não se pode manipular o conceito de 'ameaça à segurança nacional' com o fito de justificar verdadeiras violações aos direitos fundamentais.

162 A metodologia para análise de dados de inteligência dos Estados Unidos encontra empecilhos na segurança nacional, não sendo possível analisá-los com profundidade.

> É certo que os riscos, via de regra, não podem ser mensurados com precisão matemática na sociedade contemporânea, de modo que sua avaliação envolve certa dose de subjetividade, até mesmo em virtude da história recente e das peculiaridades culturais de uma sociedade específica, ensejando percepções divergentes sobre o risco (FERNANDES, 2015, v. 35, n. 2 p. 60).

Tal subjetividade implica maiores riscos à privacidade. Riscos de discriminação e, consequentemente, de erro. O maior problema dos erros preditivos é a sua invisibilidade em relação àqueles que são afetados por eles (HIRSCH, 2017, v. 14, n. 1, p. 1-9).

Como exemplo de uma atuação prejudicial por parte de governos, está a categorização de cidadãos com base em algoritmos realizada pelo Governo Polonês em 2014. Em análise da Fundação Panoptykon, realizou-se um *profiling* governamental em que os desempregados seriam divididos em três categorias de acordo com suas características pessoais, para, a partir destas categorias, serem designados os programas sociais que teriam direito.[163]

Os três perfis englobavam: 1. pessoas ativas com boas qualificações pessoais e profissionais, com 2% dos desempregados; 2. pessoas com certas qualificações profissionais, mas que não o bastante para se destacar no mercado, com 65% dos desempregados; e 3. pessoas com sérios problemas de vida que não cooperaram com a pesquisa – como pessoas deficientes e mães solteiras, com 33% dos desempregados.[164]

Percebe-se que esta política pública, ao tentar reunir perfis estigmatizados dos cidadãos desempregados, acabou por englobar 33% destes, um número considerável, na situação de, consoante o relatório, *junk people*.[165] Portanto, um terço desta população analisada seria de indesejáveis. Por isso, a categorização para fornecimento de benefícios com base na

163 PANOPTYKON FOUNDATION. **Profiling the Unemployed in Poland**: social and political implications of algorithmic decision making. 2016. p. 5. Disponível em: <https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf> Acesso em: 27 set. 2019.

164 Idem, p. 13.

165 Tradução livre: Pessoas lixo. Idem, p. 13.

automação, acabou por criar uma inevitável discriminação social.

Outro exemplo problemático sobre a possível estigmatização algorítmica, ocorreu em um julgamento de uma corte americana. No caso, Eric L. Loomis foi sentenciado a seis anos de prisão por fugir de policiais enquanto dirigia, sendo a pena calculada com base na análise automatizada de um programa. A justiça de Wisconsin utiliza o *software* COMPAS – *Correctional Offender Management Profiling for Alternative Sanctions* – um algoritmo desenvolvido por uma companhia privada que analisa a possibilidade de reincidência de um crime.[166]

O acusado apelou à segunda instância, afirmando que a utilização algorítmica retirou a sua possibilidade de um devido processo legal, principalmente por não se obter especificamente as razões pelas quais lhe foi deferida uma determinada pena.

Apesar de reconhecer estudos que afirmam que o COMPAS tem tendências a julgar com base na raça, colocando incorretamente pessoas brancas como baixo risco de reincidência,[167] a corte afirmou pela validade do sistema, já que lhe seria imposta a mesma pena mesmo que o sistema COMPAS não fosse utilizado.[168] A ressalva restou apenas como a "consideração do COMPAS é permitida; a dependência no COMPAS para a sentença imposta não é permitida".[169]

O problema, contudo, permeia o chamado por Daniel Kahneman efeito de ancoragem. Esse efeito acontece "quando as pessoas consideram um valor particular para uma quantidade desconhecida antes de estimar essa quantidade" (KAHNEMAN, 2012, p. 320). Assim, o cálculo automático da pena

166 SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. **The New York Times**. 2016. Disponível em: <https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?module=inline>.Acesso em: 27 set. 2019.

167 SUPREME COURT OF WISCONSIN. **State v. Loomis**. 881 N.W.2d 749 (Wis. 2016). p. 28. Disponível em: <http://tiny.cc/xjvidz> Acesso em: 27 set. 2019.

168 Idem, ibidem. p. 13.

169 Tradução Livre: "[...] *consideration of COMPAS is permissible; reliance on COMPAS for the sentence imposed is not permissible*". SUPREME COURT OF WISCONSIN. **State v. Loomis**. 881 N.W.2d 749 (Wis. 2016). p. 53. Disponível em: <http://tiny.cc/xjvidz> Acesso em: 27 set. 2019.

pela COMPAS pode acabar por servir de ancoragem inconsciente ao julgador.

No estudo, *Playing Dice with Criminal Sentences*, foram realizados quatro experimentos com diversos participantes, entre juízes e promotores, bem como entre pessoas leigas. Entre estudos de caso, os participantes eram enfrentados com perguntas âncoras sobre aumento de pena em 1/3 ou separados em grupos que recebiam dados viciados, tanto para mais, quanto para menos. No caso, as âncoras tanto funcionaram nos especialistas, quanto nas pessoas leigas, havendo em todos os experimentos condicionamento em relação à âncora apresentada (ENGLICH; MUSSWEILER; STRACK, 2006, v. 32, n. 2, p. 188-200).

Isto recorda fortemente a obra de Franz Kafka, *O Processo*, em que um cidadão está sendo julgado conforme critérios desconhecidos e submetido a processos e decisões a seu respeito que não possui o mínimo acesso e é incapaz de nelas interferir. Daniel Solove, ao comentar o livro juntamente com *1984*, de George Orwell, aduz que "Kafka descreve uma burocracia indiferente, onde os indivíduos são peões, sem saber o que está acontecendo, sem poder falar ou ter capacidade de exercer controle significativo sobre o processo".[170]

Por fim, o risco de **exploração** é o risco que se conecta diretamente à publicidade comportamental. Trata-se do risco da utilização dos dados para identificação de vulnerabilidades dos consumidores.

Como exemplo da exploração, Cathy O'Neil dá o exemplo de direcionamento de anúncios a jovens pobres, com a promessa de mobilidade social. Buscando lucro em aspecto vulnerável da vida do indivíduo, a Universidade de *Phoenix* investiu mais de $ 50 milhões de dólares em *Google Ads*. A partir disso, no espaço de dez anos entre 2004 e 2014, a inscrição de alunos triplicou (O'NEIL, 2016, p. 63).

Ainda há o caso do *Vatterott College*, em que foi descoberto no seu manual de recrutamento que os alvos de seus anúncios deveriam ser mulheres com filhos que recebem auxílio do governo, grávidas, recém-divorciados, pessoas com baixa autoestima, pessoas em luto, entre outras

170 Tradução livre: "*Kafka depicts an indifferent bureaucracy, where individuals are pawns, not knowing what is happening, having no say or ability to exercise meaningful control over the process*". (SOLOVE, 2004, p. 38)

situações as quais a instituição se valeria de suas fraquezas (IDEM, p. 65).

Neste caso, os anúncios predatórios foram direcionados a pessoas em necessidades com falsas e caras promessas. "Eles encontram desigualdade e se banqueteiam dela. [...] Onde quer que se encontre a combinação de grande necessidade e ignorância, você provavelmente verá anúncios predatórios" (IDEM, p. 63).

Por fim, para Dennis Hirsch, o maior desafio é arquitetar e implementar esse campo de forma a maximizar os benefícios do *big data analytics*, mas consequentemente reduzindo os seus riscos elencados.

Por vezes, as decisões tomadas com base nessa técnica são de difícil explicação, sendo tratadas ainda como a caixa-preta da inteligência artificial. Explicar o processamento de dados em determinadas topologias de redes beiram, no momento atual, à impossibilidade de explicação dos processos tomados.

Isto pode parecer absurdo em uma sociedade em que todas as respostas estão na distância de um clique, contudo, no estado da tecnologia no momento, mesmo perpassando as dificuldades postas por segredo industrial e confidencialidade, ainda não há explicações para certas correlações e resultados de processamento. A partir do *machine learning*, a inteligência artificial possui certa autonomia, podendo chegar a um resultado sem necessariamente ser desvendado como se chegou a ele.

Frank Pasquale, ao estudar a crise de 2008 em seu livro "*The Black Box Society*", ***é defensor*** da transparência algorítmica. Para o autor, a ignorância dos usuários sobre a capacidade das novas tecnologias monetiza a indústria de tecnologia em bilhões:

> Regras algorítmicas secretas para organizar informações, e guerras contra aqueles que as derrotariam, existem no *Facebook* e no *Twitter*. [...] O segredo é compreensível como estratégia de negócios, mas **destrói nossa capacidade de entender o mundo social que o Vale do Silício está criando.** Além disso, por trás da inescrutabilidade técnica, há muito espaço para conduta oportunista, exploradora e descuidada (grifos nossos).[171]

171 Tradução livre: "*Secret algorithmic rules for organizing information, and wars against those*

Portanto, a utilização cotidiana destes sistemas em certas áreas sociais ainda não é madura o suficiente. E, de toda forma, mesmo que haja a transparência no processo decisório, não significa que as decisões por ele tomadas serão legítimas. Para que a utilização de larga escala desses sistemas seja aceita, é crucial que eles sejam capazes de produzir explicações satisfatórias sobre suas decisões, mesmo sem revelar o segredo algorítmico (GILPIN, 2018, p. 1-10).

Em razão do ambiente virtual estar mais propenso a violações do direito à privacidade que no meio físico, já que naquele não se sabe exatamente quais ou o momento em que estas informações estão sendo capturadas (MENDES, 2014. p. 101-102), é indispensável uma análise mais detida nas ferramentas mais utilizadas para captura de dados pessoais e vigilância dos usuários na internet.

3.2.1 A utilização dos *cookies*, dos web *beacons*, dos *supercookies*, do HTML5 *Web Storage* e do *fingerprinting* na publicidade comportamental

Como visto, a maior pretensão para a acumulação do *big data* é a realização de correlações entre os dados e as estatísticas as quais buscam encontrar. No entanto, resta a indagação sobre de onde surgem estes dados. Em muitos casos, as coletas de dados são inerentes à própria utilização da plataforma, em que, partindo de um consentimento ou de outras bases legais, coletam-se dados para o próprio fim pactuado entre as partes: a utilização do serviço, a compra de produtos etc. No entanto, muitas vezes os dados são coletados não somente com base nesses contratos, mas sim em uma intermitente vigilância do usuário e em uma coleta massiva de suas atividades.

Nessa situação, um dado simples que geralmente não aparenta ter importância a qualquer negócio, como a compra de protetor de pisos, passa a adquirir nova dimensão. Portanto, no atual estágio de desenvolvi-

who would defeat them, exist at Facebook and Twitter, too. […] The secrecy is understandable as a business strategy, but it devastates our ability to understand the social world Silicon Valley is creating. Moreover, behind the technical inscrutability, there's plenty of room for opportunistic, exploitative, and just plain careless conduct to hide". (PASQUALE, 2015. p. 66)

mento do processamento dos dados, não existem dados sem importância (DONEDA, 2006, p. 195).

Manuel Castells (2009, p. 3), em *O Poder da Comunicação*, trata sobre a tentativa de modelar a mente humana: "Minha hipótese de trabalho é que a forma mais fundamental de poder está na capacidade de moldar a mente humana. A maneira como sentimos e pensamos determina a maneira como agirmos, tanto individual como coletivamente".[172]

Antes, em seu livro *Galáxia da Internet*, mais uma vez em referência ao livro de George Orwell, *1984*, aduz que há uma variedade de agentes que observam a casa de vidro dos cidadãos: "Não é o Big Brother, mas uma multidão de irmãzinhas, agências de vigilância e processamento de informação que registram nosso comportamento para sempre, enquanto bancos de dados nos rodeiam ao longo de toda nossa vida" (CASTELLS, 2003, p. 149).

Essas agências de vigilância fazem parte do *zero-price advertisement business model*, ou seja, um modelo de negócio que se baseia em um preço zero de publicidade que, segundo Bruno Bioni (2019, p. 33), funciona a partir da união de diversos sujeitos para a sua operacionalização, com uma complexa rede de atores que, atuando colaborativamente, atingem o objetivo final da entrega da publicidade direcionada comportamental.

As novas formas de registro se dão, principalmente, pelo monitoramento dos cliques dos usuários. O fetichismo da mercadoria de Guy Debord, transforma-se no fetichismo do clique. A partir dos cliques é possível salvar um enorme rastro de interações *on-line* para futuro uso daqueles que as decodifiquem. É o chamado *clickstream*. Este revela uma infinidade de informações sobre as preferências do usuário, de forma que a publicidade comportamental seja cada vez mais certeira. A partir dele, a publicidade direcionada na internet possui um grau de personalização jamais alcançado pela publicidade *off-line* (IDEM, p. 19).

Sobre o *clickstream*, Randal Picker afirma que a personalização de anúncios depende unicamente daquele indivíduo ao qual o anúncio é di-

172 Tradução livre: "*My working hypothesis is that the most fundamental form of power lies in the ability to shape the human mind. The way we feel and think determines the way we act, both individually and collectively*".

recionado. "Essa informação poderia surgir de qualquer número de fontes, mas o *clickstream* que nós criamos ao navegar na internet provavelmente fornece incomparável acesso à informação sobre nós" (PICKER, 2009, p. 3).

Com isso, ao ser criado pelo próprio usuário, mesmo que sem a sua ciência direta, o *clickstream* cria a sua própria biografia digital, a exemplo do que leciona Daniel Solove em *The Digital Person* (2004, p. 46):

> Nossa biografia digital é reveladora de nós mesmos, mas de uma maneira bastante padronizada. Ela consiste em *bits* de informação predefinidos e baseados no julgamento de alguma entidade sobre quais categorias de informação são relevantes ou importantes. Nós somos parcialmente capturados por detalhes como idade, raça, gênero, patrimônio líquido, propriedades e assim por diante, mas apenas de uma maneira que nos padronize tipos ou categorias. De fato, os profissionais de marketing de banco de dados frequentemente classificam consumidores em determinadas categorias baseadas em estereótipos sobre seus valores, estilo de vida e hábitos de compra. [173]

O mercado da publicidade comportamental depende dos cliques para a sua sobrevivência, não somente porque a partir deles se obtém um considerável conhecimento sobre o usuário, mas também porque os anúncios dependem dos cliques para receber as suas devidas contraprestações, como no caso do *Google Ads* (BIONI, 2019, p. 19).

Nesse cenário do *clickstream*, os *cookies* e as demais técnicas ganharam destaque na publicidade comportamental on-line ou *Online Behavioral Advertising* (OBA). Há uma terceirização do rastreamento do espaço publicitário (IDEM, p. 29). Enquanto as plataformas multilaterais veiculam os anúncios de um lado e os anunciantes que efetivamente pagam pelos anúncios estão de outro, há ainda a fundamental atuação das terceiras partes que instalam as tecnologias de monitoramento do usuário (IDEM,

173 Tradução livre: "*Our digital biography is revealing of ourselves but in a rather standardized way. It consists of bits of information pre-defined based on the judgment of some entity about what categories of information are relevant or important. We are partially captured by details such as our age, race, gender, net worth, property owned, and so on, but only in a manner that standardizes us into types or categories. Indeed, database marketers frequently classify consumers into certain categories based on stereotypes about their values, lifestyle, and purchasing habits*".

p. 29), criando uma arquitetura de monitoramento na internet.

Quanto às ferramentas de rastreamento de usuários, escolheu-se por tratar dos *cookies*, *web beacons*, *supercookies*, HTML5 *Web Storage* e *fingerprinting*, estando estas em grau crescente de caráter invasivo à privacidade do usuário. Algumas práticas possuem múltiplos nomes, optando-se em tratar principalmente pelo nome mais conhecido e disseminado na literatura.

Os ***cookies***, também conhecidos como HTTP *cookies*, hoje são peças fundamentais para a arquitetura de rede, pois viabilizam o funcionamento básico de diversos sites de internet. A possibilidade de memorização de senhas, manutenção de *login* em *sites* mais utilizados, lembrança de carrinho de compras, preferência de idiomas, entre outras funcionalidades, se dão graças aos *cookies*.

A simples visita a um *site* significa uma coleta obrigatória de certas informações sobre o visitante como endereço de IP, sistema operacional, página visitada e horário da visita.[174] Na definição de Joshua Gomez *et al.*:

> O *cookie* é um simples arquivo de texto, geralmente contendo um número de identificação único. Alguns cookies são temporários e outros podem ser retidos no disco rígido e utilizados em várias visitas. Se o site exigir informações de login ou de registro, ele poderá correlacionar informações de identificação pessoal (PII) com o comportamento da navegação.[175]

Esta definição está relacionada à utilização típica dos *cookies* no rastreamento realizado pelas primeiras partes, ou seja, os *sites* em que o usuário ativamente e voluntariamente visita.

Os *cookies*, contudo, possuem a função mais popularizada em sua utilização atípica, que se relaciona diretamente ao rastreamento por terceiras partes, que inserem seus *cookies* para vigilância. O rastreamento pelas ter-

174 GOMEZ, Joshua; PINNICK, Travis; SOLTANI, Ashkan. *Know Privacy*. Relatório da Universidade de Berkeley. Disponível em: <http://knowprivacy.org/full_report.html> Acesso em: 29 set. 2019.

175 Tradução livre: "*The cookie is a simple text file, usually containing a unique identifying number. Some cookies are temporary and some may be retained on the hard drive and used for multiple visits. If the website requires login or registration information, it can correlate personally identifiable information (PII) with browsing behavior*". Idem, p. 8.

ceiras partes não mantém uma relação direta com o usuário e, por consequência, é invisível a eles (BIONI, 2019, p. 29).

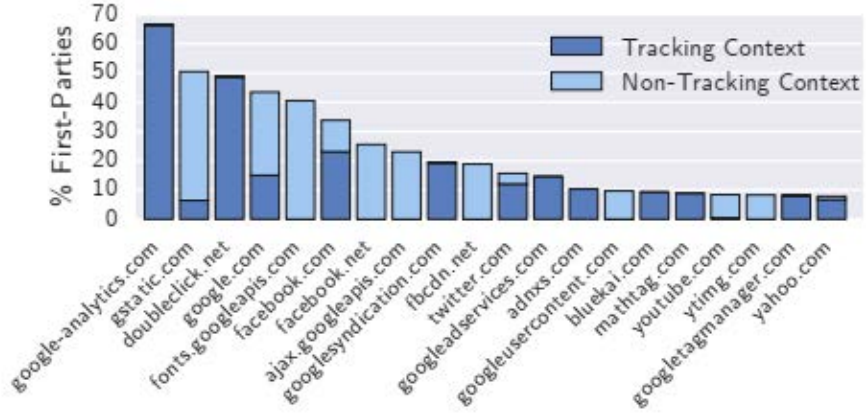
Portanto, as imagens de anúncios que geralmente se vê em *sites* não são fornecidas diretamente do operador do *site*, mas sim a partir das *advertising networks*.[176] Essas redes são empresas que vendem anúncios em nome dos *sites* visitados. No processo de visita aos *sites* que se suprem monetariamente a partir dos seus anúncios, as primeiras partes, como é o caso da versão *on-line* de muitos jornais, há a colocação de *cookies* na máquina do usuário pelas primeiras e terceiras partes. Assim, como a barra de anúncios não é fornecida diretamente pelo site principal, é possível que haja a perseguição de mesmos anúncios ao longo de diversos sites da rede.

Os pesquisadores Steven Englehardt e Arvind Narayanan (2016, p. 2), ao analisar mais de um milhão de sites em suas práticas adotadas para rastreamento *on-line*, indicam que as terceiras partes podem facilmente obter o histórico de navegação dos usuários a partir de uma combinação de *cookies* e outras tecnologias, de forma a identificar unicamente aquele usuário, bem como obter seu endereço de e-mail e outras informações sensíveis. Os *sites* escolhidos se deram a partir da listagem de sites com popularidade global consoante pesquisas realizadas no dispositivo da *Amazon Alexa*.

Ao tentar quantificar o número de terceiras partes atuantes no ambiente da *web*, eles obtiveram a existência de 81.000 delas. Contudo, apenas 123 terceiras partes daquele total estão presentes em mais de 1% dos sites, ou seja, as terceiras partes encontradas cotidianamente são significantemente as mesmas. *Google, Facebook, Twitter e AdNexus são as únicas terceiras partes presentes em mais de 10% dos sites* (IDEM, p. 8), consoante análise do gráfico abaixo:

176 GOMEZ, Joshua; PINNICK, Travis; SOLTANI, Ashkan. Op. cit. p. 8.

FIGURA 9 – TOP TERCEIRAS PARTES NOS PRINCIPAIS 1 MILHÃO DE SITES



Fonte: ENGLEHARDT, Steven, NARAYANAN, Arvind. Online tracking: A 1-million-site measurement and analysis. *In*: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, October 24-28, 2016, Vienna, Áustria, doi: 10.1145/2976749.2978313, p. 08. Disponível em: <http://bit.do/fa6PJ>. Acesso em: 29 set. 2019.

Mais uma vez, verifica-se a dominância do ambiente digital por poucos jogadores.

Os ***web beacons***, conhecidos também por *web bugs*, *clear GIFs* e *pixel tags*, não são utilizados unicamente como ferramentas de publicidade comportamental, sendo colocados no código HTML das páginas visitadas para visualizar o histórico de quem está acessando a página, de forma a criar um perfil das páginas que a pessoa está visitando.[177] Mesmo que o usuário elimine os *cookies* armazenados, os *web beacons* ainda possuem a capacidade de rastrear a navegação do usuário por meio de seu IP.

A escolha de não monitoramento pelos *web beacons* é mais complexa que as dos *cookies*, segundo Joshua Gomez *et al*, já que apenas bloquear os *cookies* das terceiras partes não impede o monitoramento e, mesmo que se

177 GOMEZ, Joshua; PINNICK, Travis; SOLTANI, Ashkan. **Know Privacy**. Relatório da Universidade de Berkeley. Disponível em: <http://knowprivacy.org/full_report.html>. Acesso em: 29 set. 2019.

instale bloqueadores de conteúdo das terceiras partes, esta solução traria prejuízos à própria navegação do usuário.[178]

Os ***supercookies***, também chamados de *flash cookies*, foram criados a partir da ciência das redes de anúncios que 30% usuários deletavam mensalmente seus HTTP *cookies* (SOLTANI et al., 2009, p. 1). Com grandes semelhanças entre eles, apesar de possuírem nomes mais peculiares, podem ser incluídos em sua mesma categoria os *evercookies* (*cookies* zumbis), um *cookie* persistente à tentativa de ser deletado pelo usuário e, da mesma forma, o *Flash Local Shared Objects* (LSOs). Com isso, os *supercookies* foram criados, incluindo diversos benefícios àqueles que pretendem monitorar o usuário, como: maior capacidade de armazenamento de informação (100KB em vez de 4KB dos HTTP *cookies*), ausência de data de validade, diferentemente da maioria dos *cookies*, que expiram ao fim de uma sessão e seu armazenamento ocorre em lugar diferente dos *cookies*, dificultando ao usuário que os encontrem (IDEM, p. 1).

Para Ashkan Soltani *et al.*, essas diferenças implicam que os "Flash cookies são uma tecnologia mais resiliente ao rastreio que os HTTP cookies, criando uma área para incertezas no controle de privacidade pelo usuário".[179] Estes engenheiros descobriram, em 2009, que *supercookies* foram criados com a pretensão de reviver um HTTP *cookie* após a atuação afirmativa do usuário em removê-lo.

Além de problemas de privacidade, implicam em desrespeito à autodeterminação do usuário em manter ou não rastros das suas atividades em seu navegador, já que, mesmo excluindo o conteúdo dos seus *cookies*, estes podem ser totalmente revitalizados a qualquer momento.

Um pouco mais sofisticado que os *supercookies*, apesar de poder ser incluído em seu espectro, destaca-se o *HTML5* **Web Storage**. Enquanto os *supercookies* possuem uma abordagem efêmera, os HTML5 são mais persistentes. Um grande melhoramento é a capacidade de armazenamento

178 GOMEZ, Joshua; PINNICK, Travis; SOLTANI, Ashkan. **Know Privacy**. Relatório da Universidade de Berkeley. p. 9. Disponível em: <http://knowprivacy.org/full_report.html> Acesso em: 29 set. 2019.

179 Tradução livre: "*These differences make Flash cookies a more resilient technology for tracking than HTTP cookies, and creates an area for uncertainty for user privacy control*" (SOLTANI et al., 2009, p. 1).

– enquanto 100KB para os *flash cookies*, possuem 5Mb de espaço.

Consoante Ashkan Soltani *et al* (2012, p. 284), complementando o trabalho anterior, os HTML5 foram amplamente detectados em sites como *Hulu*, *CNN* e *Twitter*, possuindo maior utilização que os *cookies* e os *flash cookies*. Como razão da sua melhor adaptação ao monitoramento está a ausência de necessidade de utilização de *plug-ins* com *Flash* instalados no computador do usuário.

Outro monitoramento é por meio do ***fingerprinting***, que, assim como o nome já sugere, é altamente intrusivo, captando aspectos sensíveis do usuário, ou seja, uma impressão digital no digital. Similarmente aos *cookies*, mas de forma mais singular, é possível a captação de informações sobre fuso-horário, fontes utilizadas, resolução da tela, *plug-ins* instalados, idioma etc. Para Steven Englehardt e Arvind Narayanan (2016), o *fingerprinting* é uma forma de rastreamento persistente que não requer qualquer configuração ou instalação no *browser* do usuário. Além disso, é uma técnica muito difícil de ser rastreada, já que não deixa evidências no computador do usuário (ECKERSLEY, 2010, p. 3).

O *fingerprinting não compreende necessariamente* uma técnica de rastreamento, sendo conjuntos de técnicas que identificam o usuário sem a instalação de *cookies*, partindo das propriedades do seu sistema e *browser*.

Esta técnica é similar à regeneração de *cookies*, mas, além disso, consoante afirma Peter Eckersley, "uma fingerprint que carrega não mais que 15-20 bits de informação identificadores será em quase todos os casos suficiente para identificar unicamente um browser em particular, a partir do seu endereço de IP, sua subnet ou até mesmo seu ASN" (IDEM, p. 3).[180] [181] Em sua pesquisa na *Electronic Frontier Foundation*, foi estabelecido um algoritmo de *fingerprinting* no site do projeto *Panopticlick* e, a partir de 470.161

180 Tradução livre: *"[...] a fingerprint that carries no more than 15-20 bits of identifying information will in almost all cases be sufficient to uniquely identify a particular browser, given its IP address, its subnet, or even just its Autonomous System Number*". (ECKERSLEY, 2010, p. 3).

181 Definição de Autonomous System Number: "*An autonomous system number (ASN) is a unique number that's available globally to identify an autonomous system and which enables that system to exchange exterior routing information with other neighboring autonomous systems*". AUTONOMOUS System Number (ASN). **Techopedia**. Disponível em: <https://www.techopedia.com/definition/26871/autonomous-system-number-asn>. Acesso em: 30 set. 2019.

navegadores participantes em visitas neste site, foi possível o estabelecimento de *fingerprints* para 83,6% dos *browsers* (IDEM, p. 8).

Mesmo que a impressão digital do usuário se alterasse pelo uso contínuo e mudanças de preferências em *sites*, foi implementado um simples algoritmo para estimar a evolução dessa impressão, o qual foi capaz de identificar em 99,1% dos casos uma correta evolução da mesma impressão digital (IDEM, p. 13).

Com isso, a técnica do *fingerprinting* é em grande parte maliciosa porque realizada para rastrear diretamente as pessoas que, no exercício do seu direito à privacidade, limitam a ação dos *cookies*. Sem o controle e conhecimento do usuário, essas práticas parecem ser mais assustadoras do que úteis. Em verdade, demonstra-se que o *fingerprinting* não oferece nenhuma funcionalidade ao usuário, criando inclusive um potencial identificador global em que se pode acompanhar a navegação dos usuários, para, após, realizar o direcionamento de publicidade a partir dos perfis criados (ECKERSLEY, 2010, p. 3).

De forma a analisar essas funcionalidades que pretensamente buscam o máximo de lucros para os negócios de transações de dados, Omer Tene e Jules Polonetsky escreveram o artigo "*A Theory of Creepy: Technology, Privacy, and Shifting Social Norms*". Para os autores, uma forma de evitar as atuações intrusivas e bizarras da tecnologia é propriamente evitar o determinismo tecnológico. Ou seja, mesmo que o estado da arte esteja avançado o suficiente para que algo seja possível, não significa que ele deva ser feito (TENE; POLONETSKY, 2014, v. 16, n. 1, p. 83).

A reflexão, portanto, é sobre a capacidade de impermanência do mundo físico, ao contrário do que ocorre no mundo digital. Por exemplo, tem-se uma noção de que um livro deve ser mais permanente e definidor do caráter de um autor que suas notas em *post-its* ou seus rascunhos de ideias. Contudo, transpondo a relação para o mundo digital, os rascunhos se assemelham aos e-mails, *tweets*, que, *a priori*, não são feitos para possuir uma permanência na história de alguém, mas na internet seus rastros são quase impossíveis de conter, rastrear e destruir (IDEM, p. 84).

Omer Tene e Jules Polonetsky concluem que não deve haver o contentamento com a simples resposta "é assim que a tecnologia funciona". A projeção de novas tecnologias deve, ao invés disso, ocupar-se dos valores

sociais como guias determinantes para a atuação tecnológica (IDEM, p. 84).

A lógica de acumular por acumular no mundo físico é visto como insana e "antissustentável", mesmo que o indivíduo possua meios para tanto. É preciso transpor essa lógica para o mundo digital.

Stefano Rodotà (2008, p. 20) faz uma associação direta do impacto sobre a privacidade com o impacto ambiental. Para o autor, é necessária a introdução e procedimentos que avaliem o impacto da privacidade pois o desgaste das liberdades civis não é menos importante que o desgaste ambiental.

Laura Schertel também realiza uma comparação à preservação ambiental. Assim como há o desenvolvimento sustentável em matéria ambiental, a sociedade somente "poderá obter as vantagens do desenvolvimento tecnológico se este for acompanhado da tutela jurídica da privacidade" (MENDES, 2014, p. 34).

A partir dessa acumulação desenfreada é que surgem os *data brokers* que criam um perfil de um indivíduo por meio de diversos pedacinhos de informação de bases de dados públicas e privadas, para continuamente vender e reutilizar os dados pessoais dos indivíduos (BIONI, 2019, p. 30).

Um famoso *data broker* no Brasil é o *Mosaic* Brasil, produto do *Serasa Experian*, plataforma que, consoante própria definição, "classifica a população brasileira em 11 grupos e 40 segmentos, considerando aspectos financeiros, geográficos, demográficos e comportamentais, consumo e estilo de vida".[182] Estes grupos vão de A a K, sendo A elites brasileiras, passando por massa trabalhadora urbana, habitantes de zonas precárias, e o grupo K, habitantes de áreas rurais.

Cathy O'Neil traz um exemplo sobre como os rastros digitais podem negativamente influenciar o mundo físico. No caso, Helen Stokes buscava vaga em um asilo comunitário, mas era continuamente rejeitada pelo sistema por possuir registros de prisão. As prisões, contudo, provinham de brigas com seu antigo marido, não sendo ela condenada como culpada e, por isso, sequer possuindo antecedentes criminais nos registros governamentais. Contudo, os registros de prisão continuavam na base de dados de uma companhia privada *RealPage*. Helen apenas conseguiu limpar seus

182 Visão Geral da apresentação do Mosaic Brasil. Disponível em: <https://www.serasaexperian.co m.br/produtos/mosaic> Acesso em: 29 set. 2019.

registros após um processo judicial, o que não se espera que seja levado a cabo por milhares de cidadãos alvos desses registros (O'NEIL, 2016, p. 127).

Essas ferramentas de *data exchange* são plataformas em que anunciantes dão lances para acessar dados dos consumidores, sendo estes dados provenientes de rastreio *on-line* ou *off-line,* possivelmente já estratificados em perfis comportamentais determinados. A partir disto, consoante relatório da OCDE, *Exploring the Economics of Personal Data*,

> Vinculando isso [perfil comportamental] ao código de identificação único incorporado aos cookies no computador ou dispositivo portátil do usuário, um anunciante pode direcionar anúncios para o usuário em particular e/ou simplesmente comprar espaço publicitário em sites que correspondam aos interesses desse perfil de usuário por meio de uma troca de publicidade. Com isso, entrega-se anúncios a usuários que provavelmente se interessarão por eles.[183]

Outro famoso *marketplace* de *data exchange* é o *BlueKai* do *Oracle*, que, em 2013, possuía dados de mais de 300 milhões de usuários, oferecendo mais de 30.000 atributos de dados, processando mais de 750 milhões de dados e leiloando mais de 75 milhões de informações pessoais por dia.[184]

Nesse contexto de massiva datificação, um usuário que pretenda evitar a vigilância na *web* de forma efetiva deve ser capaz de passar por três testes. O primeiro é o mais simples: encontrar as configurações apropriadas que permitem os *cookies* em sua utilização típica e necessária, bloqueando aqueles que tentem um rastreamento indesejado. O segundo é mais complicado: aprender sobre todos os tipos de *supercookies*, entre estes alguns tipos obscuros, encontrando maneiras de desativá-los. Apenas uma

183 Tradução livre. "*Linking this to the unique identification code embedded in cookies on the user's computer or handheld device, an advertiser can target advertisements at the particular user, and/or simply buy advertising space on websites matching the interests of that user profile through an advertising exchange. Thus delivering advertisements to users who are likely to be interested in them*". ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. Exploring the Economics of Personal Data. **OECD Digital Economy Papers**, [s.l.]. p.1-39, 2 abr. 2013. p. 14. Disponível em: <http://dx.doi.org/10.1787/5k486qtxldmq-en>. Acesso em: 30 set. 2019.

184 Idem, p. 15.

minoria passaria pelo segundo teste, para ser, enfim, confrontada com um terceiro desafio: evitar formas de *fingerprinting* (ECKERSLEY, 2010, p.3).

Como muitas vezes os usuários, por si, não são capazes de conter o massivo rastreamento, surgem as *Privacy Enhancing Technologies* (PETs),[185] de forma a permitir uma maneira em potencial de proteção da sua privacidade.

Para Peter Eckersley, criador dos três testes anteriores, o Projeto Tor é um bom navegador que já possui desenvolvimento contra os riscos de *fingerprinting*, sendo uma das poucas formas que é capaz de evitá-la (ECKERSLEY, 2010, p. 16).

Como uma PET, o Tor é um *software* de código aberto que é acrônimo para "*The Onion Router*", roteamento cebola que permite, a partir da difusão do sinal do usuário em diversos servidores voluntários, o anonimato, sendo utilizado em grande parte por ativistas de direitos humanos perseguidos. Foi ferramenta utilizada durante a primavera árabe, bem como para operacionalização das denúncias de Edward Snowden em 2013.[186]

Há ainda as ferramentas de *Do Not Track* (DNT), cuja maior dificuldade no momento é a implementação e o *enforcement*. Existem alguns softwares que as fornecem, mas de forma aleatória e não regulamentada. Além disso, nem todas essas possuem a capacidade de tornar a navegação extremamente segura para o usuário ao mesmo tempo que a torna fácil e eficaz.

Steven Englehardt e Arvind Narayanan, analisando a efetividade das *PETs* de *DNT*, como a ferramenta própria do navegador *Firefox* de bloquear *cookies* de terceiras partes, verificaram que apenas 0,4% dos *sites*, do total de 1 milhão da análise, foram capazes de incluir *cookies* de terceiras partes enquanto ativado o bloqueador do Firefox. No mesmo sentido, com a ferramenta *Ghostery* obteve-se um bom resultado de 0,3% (ENGLEHARDT; NARAYANAN, 2016, p. 10).

Contudo, a análise acima deu-se apenas em face dos *cookies*, que é a prática de rastreio mais facilmente perceptível e bloqueável, não analisando também a capacidade de um usuário médio ao habilitar e programar a *PET*.

Assim, Pedro Leon, Lorri Cranor *et al.* (2012, p. 10), pesquisadores da

185 Algumas PETs já foram introduzidas no primeiro capítulo, subseção 2.4.5.

186 Sobre o Projeto Tor. Disponível em: <https://www.torproject.org/pt-BR/about/history/> Acesso em: 30 set. 2019.

Universidade Carnegie Mellon, estudaram a usabilidade das ferramentas que buscam limitar a *OBA* por usuários médios. Eles observaram o comportamento e a percepção de 45 participantes ao baixar, instalar e configurar nove ferramentas de privacidade, encontrando sérios problemas que esbarram na efetividade dessas ferramentas. Estes participantes eram pessoas com educação significativa, entre 19 e 57 anos, sem experiência em ciência da computação ou em desenvolvimento da *web*. Segundo os autores:

> Encontramos sérias falhas de usabilidade nas nove ferramentas avaliadas, demonstrando que o seu *status quo* é insuficiente para permitir que os usuários protejam sua privacidade. Embora reconheçamos que o setor de publicidade, fornecedores de navegadores, e terceiras partes tenham contribuído com uma variedade de ferramentas para esse ecossistema, **nós encorajamos uma ênfase maior na usabilidade em futuros desenvolvimentos** (grifos nossos).[187]

Quanto à possibilidade de fazer escolhas significativas quanto ao rastreamento em si, foi um tema amplamente debatido na Uni*ão Europeia. Havia, principalmente, duas correntes*, os sistemas *opt-in* e *opt-out*. A primeira, *opt-in*, defendeu que o titular dos dados pessoais deveria consentir previamente e expressamente, aceitando cada *cookie* a ser instalado na navegação. A segunda destaca o consentimento posterior, já que a escolha do usuário poderia ser feita *a posteriori*. A partir da extração das suas configurações dos *browsers* e exclusão dos *cookies* instalados (*opt-out*) (BIONI, 2019, p. 178).

187 Os autores continuam: "Existem desafios significativos no fornecimento de ferramentas fáceis de usar, que oferecem aos usuários controle significativo, sem interferir no uso da Web. [...] **Mesmo com educação adicional e melhores interfaces de usuário, não está claro se os usuários são capazes de fazer escolhas significativas sobre os rastreadores**". Tradução livre: "*We found serious usability flaws in all nine tools evaluated, demonstrating that the status quo is insufficient for empowering users to protect their privacy. While we recognize that the advertising industry, browser vendors, and third parties have contributed an assortment of tools to this ecosystem, we encourage a greater emphasis on usability moving forward.* [...] *There are significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web.* [...] *Even with additional education and better user interfaces, it is not clear whether users are capable of making meaningful choices about trackers".* (LEON et al., 2012, p. 10)

Após as discussões, por meio da Diretiva 2009/136/CE houve alteração da Diretiva 2002/58/CE, que trata da privacidade nas comunicações eletrônicas, determinando a necessidade de consentimento prévio do usuário para qualquer tentativa de coleta de informações, envolvendo nisto os *cookies*, sendo uma clara adesão ao sistema *opt-in*. (MENDES, 2014, p. 103).

O GDPR confirmou a vigência da diretiva 2002/58/CE em seu em seu art. 95,[188] bem como no considerando 173,[189] estabelecendo que ela deve ser alterada em conformidade com o regulamento.

Contudo, para Bruno Bioni, o sistema *opt-in* se revelou com um efeito adverso inesperado, já que como se exigia um consentimento prévio e expresso, os usuários receberam uma avalanche de pedidos de permissões para a instalação dos *cookies*. Todos esses *disclaimers* tornaram a navegação do usuário maçante, bem como com a obtenção de um consentimento impensado e automático (BIONI, 2019, p. 178).

O autor continua: "De nada adianta preceituar uma gama ampla de qualificadores para o consentimento, acompanhada de um debate binário se ele deve ser prévio (*opt-in*) ou *a posteriori* (*opt-out*), se não há um movimento de regulação para efetivar esse direito" (IDEM, p. 182).

É interessante ressaltar que algumas empresas como o *Google*, o *Instagram* e o *Facebook*, amostras de grandes acumuladoras de dados pessoais, permitem uma personalização pelo próprio usuário sobre os anúncios visualizados, possibilitando opções de parar de ver o anúncio ou informar que aquele lhe incomoda. Não se sabe ao certo até que ponto

188 O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE.

189 (173) O presente regulamento deverá aplicar-se a todas as matérias relacionadas com a defesa dos direitos e das liberdades fundamentais em relação ao tratamento de dados pessoais, não sujeitas a obrigações específicas com o mesmo objetivo, enunciadas na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, incluindo as obrigações que incumbem ao responsável pelo tratamento e os direitos das pessoas singulares. A fim de clarificar a relação entre o presente regulamento e a Diretiva 2002/58/CE, esta última deverá ser alterada em conformidade. Uma vez adotado o presente regulamento, a Diretiva 2002/58/CE deverá ser revista, em especial a fim de assegurar a coerência com o presente regulamento.

a opção do usuário em relação a publicidade direcionada é levada em conta pelas empresas.

Ainda, o *Facebook* possui a ferramenta "Por que estou vendo isto?", em que a rede social apresenta motivos sobre o porquê de se ver certos anúncios. Contudo, não se pode esperar que a plataforma realmente revele todas as razões que fomentaram um anúncio, já que, por toda a estruturação de *likes* e interesses, o Facebook tende a demonstrar saber demasiadamente sobre os perfis de seus usuários, mesmo que não apresente as específicas correlações.

Uma forma encontrada para tornar a experiência dos usuários menos maçante, mas ao mesmo tempo mais protegida, é a utilização de *nudges* também na privacidade desde a concepção. A noção de *nudges* foi inicialmente inserida na literatura por Richard Thaler e Cass Sunstein, rendendo àquele o prêmio Nobel de economia em 2017. É uma noção sobre a arquitetura de escolhas, bem como como estas podem ser condicionadas com um simples rearranjo da estrutura (THALER; SUNSTEIN, 2009).

Nudges são soluções levemente paternalistas, constituindo microincentivos que levam a uma mudança de comportamento, podendo serem capazes de condicionar o comportamento à proteção da privacidade. Para os autores, os *nudges* são "qualquer aspecto da arquitetura de escolha que altera o comportamento das pessoas em um modo previsível sem proibir quaisquer opções ou mudar significativamente seus incentivos econômicos [...]" (IDEM, p. 6).

Para Lorrie Cranor *et al.*, as inserções dos *nudges* para aprimoramento da privacidade na internet evitam formas de coerção, tornando a experiência dos usuários além de leve, segura. Enquanto alguns *nudges* seriam apenas para a informação do usuário, outros buscam alterar a percepção individual dos custos e benefícios dos compartilhamentos das informações pessoais (BALEBAKO et al., 2011, p. 2).

Em um estudo de 2013, pesquisadores buscaram inserir três *nudges* na navegação do *Facebook*. No primeiro, haveria indicações visuais de qual seria a audiência de algum *post*, no segundo, inseriu-se um *delay* antes da publicação de um post possibilitando editar conteúdo ou cancelar o envio e, por último, dá-se *feedback* aos usuários sobre os efeitos de suas publicações.

FIGURA 10 – *NUDGE* DA AUDIÊNCIA EM POTENCIAL

Fonte: WANG, Yang et al. Privacy nudges for social media. **Proceedings Of The 22nd International Conference On World Wide Web – Www '13 Companion**, [s.l.], p.1-8, 2013, p. 02. Disponível em: <http://tiny.cc/tzd0dz>. Acesso em: 05 out. 2019.

Partindo da premissa de que geralmente os usuários do Facebook não se atentam para quem poderá ver suas publicações, as imagens servem de lembrete sobre quem verá o conteúdo, de forma a evitar futuros arrependimentos. Na pesquisa com 21 participantes que instalaram o *plug-in*, vários destes indicaram que, sabendo das pessoas que possivelmente veriam os *posts*, repensaram a publicação.

Em relação ao *nudge* de tempo, em vez, alguns participantes acharam irritante esperar pela publicação ser enviada, contudo, a maioria encontrou utilidade já que nesse tempo conseguiam reler o que escreveram, reformulando frases ou retirando palavrões. Quanto ao *nudge* de sentimento, este foi o de funcionamento mais "inacurado", pois, por vezes, indicava sentimentos fora de contexto. De toda forma, fez uma usuária repensar a utilização de um palavrão (WANG et al., 2013, p. 6).

Essa experiência revelou que alguns *nudges* de privacidade podem ser levados em conta para arquitetar uma cultura de proteção à intimidade, bem como evitar arrependimentos em publicações na internet.

Apesar da existências das *PETs*, indispensável notar que para que elas efetivamente protejam o usuário as ferramentas devem ser usáveis, no sentido de que um usuário médio facilmente compreenda quais opções de monitoramento pode aceitar ou não. A utilização descontrolada

de dados pessoais já causou danos e prejuízos em inúmeras situações e, caso não haja a devida conscientização de todas as partes envolvidas na multilateralidade da internet, esta pode se tornar um ambiente hostil aos direitos do consumidor e aos direitos humanos.

3.3 Análise dos casos de coletas de dados para direcionamento de publicidade comportamental com prejuízo aos usuários

Como principal insumo no mundo digital, os dados movimentam a economia de forma nunca vista. Os dados pessoais possuem um viés marcadamente dinâmico, permitindo que estes manejem a informação, relacionando e reelaborando dados, sendo capaz de tirar, a partir disso, conclusões (MENDES, 2014, p. 58).

A problemática abrange as conclusões tiradas de uma análise puramente "dataísta". Problemas de vieses, de erros, de privacidade e de discriminação, consoante diversos casos já comentados brevemente, apelam diretamente ao tipo de personalidade que se pretende "datificar", possuindo consequências possivelmente irreparáveis para os afetados.

A inclusão digital ainda não é uma realidade global e, algumas técnicas como excluir *cookies*, visitar sites em modo anônimo e buscar ferramentas de DNT, são tarefas difíceis para uma maioria dos usuários brasileiros. Nisto, o risco de manipulação se acentua.

Estes casos demonstram que, à exemplo da teorização de Shoshana Zuboff, deve-se ter a certeza de combater o capitalismo de vigilância, não a tecnologia em si (ZUBOFF, 2019, Cap. 1, paginação irregular). A comoção ocorrida com a descoberta de métodos da *Cambridge Analytica* acabou por inserir na sociedade um despertar para a importância de se resguardar direitos dos titulares também no ambiente *on-line*.

O credo do criador do *Facebook* "*move fast and break things*"[190] não

190 Trecho da carta de Mark Zuckerberg aos seus potenciais investidores: "*We have a saying: 'Move fast and break things.' The idea is that if you never break anything, you're probably not moving fast enough*". MARK Zuckerberg's Letter to Investors: 'The Hacker Way'. **Wired**. 2012. Disponível em: <https://www.wired.com/2012/02/zuck-letter/>. Acesso em: 1º out. 2019.

mais se coaduna com a expectativa dos usuários da atuação de plataformas no ambiente *on-line*. Ainda o seu "*hacker way*",[191] copiado pela maioria das empresas do Vale do Silício, em que pretensamente envolve contínuo melhoramento e interação da experiência, provou-se uma experiência desastrosa em termos de proteção da privacidade e de manipulações externas.

Optou-se por excluir o célebre caso do direcionamento de publicidade política da *Cambridge Analytica* – já comentado brevemente na subseção 2.3 – por não envolver diretamente serviços direcionados a consumidores, possuindo, mais implicações propriamente democráticas.

Apesar de infelizmente existirem inúmeras situações de criação de perfis comportamentais de usuários na internet, destacaram-se casos paradigmáticos com demasiados riscos de manipulação de dados para *profiling*, bem como riscos de exploração e à privacidade dos usuários.

Em cada tópico abaixo, haverá um histórico do caso, bem como seus desdobramentos. A documentação destes é relevante para buscar ferramentas para prevenir situações futuras, de forma a preservar a livre determinação dos usuários enquanto cidadãos no mundo digital.

3.3.1 A empresa Target e as previsões de gravidez

Talvez, um dos casos mais comentados sobre a utilização do *big data analytics* na publicidade comportamental é o da empresa *Target* e a sua previsão de gravidez em uma adolescente. É o único caso de publicidade direcionada *off-line* a ser comentado, por meio de propagandas impressas, mas que possui grandes reflexos da correlação em análises de dados automatizadas.

Percebendo desde cedo a capacidade de processamento em análise

191 "*We have cultivated a unique culture and management approach that we call the Hacker Way. […] The Hacker Way is an approach to building that involves continuous improvement and iteration. Hackers believe that something can always be better, and that nothing is ever complete. They just have to go fix it – often in the face of people who say it's impossible or are content with the status quo*". MARK, Zuckerberg's Letter to Investors: 'The Hacker Way'. **Wired**. 2012. Disponível em: <https://www.wired.com/2012/02/zuck-letter/>. Acesso em: 1º out. 2019.

de dados, a empresa varejista passou a se debruçar nas correlações das análises de dados, especialmente por meio do seu funcionário Andrew Pole, matemático e estatístico. Andrew foi o responsável em explicar ao mundo como a empresa previu a gravidez, sendo noticiado pelo jornalista Charles Duhigg no jornal *The New York Times*.

Conseguiu-se identificar, a partir dos departamentos de *marketing* das empresas deste ramo, que, geralmente, os clientes não compram tudo o que precisam em apenas uma loja, mesmo que ela tenha a possibilidade de lhes suprir todas as necessidades. Ao invés disso, diversificam as compras em diversos estabelecimentos, como alimentos em supermercados, brinquedos nas lojas de brinquedos etc. A *Target* possuía a difícil missão de convencer os fregueses de realizar todas as suas compras em sua loja, assim o desafio era mudar estes comportamentos quando os hábitos de consumo já estão concretizados (DUHIGG, 2012).

Com isso, em seus intensos estudos, descobriu-se que há breves momentos na vida em que todos os hábitos da pessoa se desconstroem, criando de forma rápida e intensa novos hábitos. Nessas fases marcantes de vida estão ter filhos, mudar de cidade, entrar na universidade e conseguir um novo emprego. Assim, captar o consumidor neste momento significa grandes chances de estes continuarem clientes fiéis.

Partindo desses grandes momentos da vida, a empresa focou-se especificamente no nascimento de novos membros da família. Contudo, não bastava atingir os pais quando o bebê já tivesse nascido, já que concorrentes já poderiam ter conquistado sua lealdade. No caso, *timing* é essencial. A *Target* queria atingir as mulheres ainda grávidas, especialmente no segundo trimestre de gravidez, quando as grandes compras possivelmente ainda não haviam sido realizadas.

Consoante Andrew Pole:

> Nós sabíamos que se pudéssemos identificá-las no segundo trimestre, haveria uma boa chance de capturá-las por anos', disse-me Pole. "Assim que conseguirmos que elas comprem nossas fraldas, elas começarão a comprar todo o resto também. Se você está correndo pela loja, procurando garrafas e passa por um suco de laranja, você pega uma caixa. Ah, e tem esse novo DVD que eu quero. Em breve,

> você estará comprando nossos cereais e toalhas de papel e continuará voltando.[192]

Por décadas, a *Target* coletou dados de consumo de seus clientes, catalogando-os por meio de um *Guest ID*. Com isso, saberiam que deveriam enviar cupons de protetor solar em julho (verão americano) para os clientes que compraram roupas de banho em abril.

A partir da análise dos *Guest ID* dessas grávidas, buscaram correlações: o que as grávidas compram que as não grávidas não compram? A correlação para identificar as clientes grávidas foi encontrada na análise da mudança de hábitos quando o parto se aproxima. E o parto poderia ser previsto, pois, ao ter registros de listas de chá de bebê, sabe-se que, após alguns meses do chá, um parto aconteceria.

Perceberam que as grávidas comprariam mais cremes inodoros no começo do segundo trimestre de gravidez e que mulheres de até vinte semanas comprariam muitos suplementos de cálcio, magnésio e zinco.[193] Assim, chegaram a uma lista de 25 produtos que, analisados em contexto, forneciam um *score* de gravidez. Ainda, o parto era previsto, possibilitando que os cupons de desconto fossem enviados à cada etapa específica da gravidez.

Andrew Pole conta, em sua entrevista, uma história não identificada, "anonimizada", de uma consumidora adolescente. Essa história foi, então, reproduzida na matéria do *The New York Times*, sendo recontada e reproduzida diversas vezes em livros[194] e palestras.[195] Vale ressaltar que nunca

192 Tradução livre: "*We knew that if we could identify them in their second trimester, there's a good chance we could capture them for years," Pole told me. "As soon as we get them buying diapers from us, they're going to start buying everything else too. If you're rushing through the store, looking for bottles, and you pass orange juice, you'll grab a carton. Oh, and there's that new DVD I want. Soon, you'll be buying cereal and paper towels from us, and keep coming back*". (DUHIGG, 2012)

193 IDEM.

194 Cf. Bioni (2019, p. 42); Tene (2014, v. 16, n. 1 p. 66); e Cukier e Mayer-Schoenberger (2013, paginação irregular)

195 HIRSCH, Dennis. Keynote 2 – Além do controle: reinventando a lei de privacidade para a economia algorítmica. In: *10º Seminário de Proteção à Privacidade aos Dados Pessoais.* São Paulo, 2019. Disponível em: <https://www.youtube.com/watch?v=YMoXqvNhFSw&t=5852s> Acesso em: 1º out. 2019.

houve a confirmação por alguma parte envolvida ou algum procedimento judicial que a envolvesse.

No caso relatado, um homem compareceu a uma *Target* próximo a Mineápolis buscando o gerente. Cupons de desconto relativos a objetos de gravidez, roupas maternas e móveis de bebês foram enviados à sua filha que ainda estava no ensino médio. O pai, então, culpava a companhia de estimular jovens adolescentes a engravidarem.

A empresa, tentando desculpar-se com a família, algumas semanas após o ocorrido realizou uma ligação, momento em que, na verdade, o pai da jovem que se desculpou, uma vez que a gravidez de sua filha era uma realidade, com o parto previsto para agosto (DUHIGG, 2012).

Eric Siegel, também entrevistado na matéria do *The New York Times*, afirma em seu livro *Predictive Analytics: the power to predict who will click, buy, lie, or die* que, dois anos antes da reportagem, Andrew Pole revelou essa mesma história em uma palestra que ele assistia, não havendo qualquer ar de reprovação pela plateia. Contudo, após a matéria de Charles Duhigg, o caso viralizou de forma negativa:

> Um ano depois, em fevereiro de 2012, Duhigg publicou um artigo de primeira página na revista *New York Times*, provocando um surto viral que transformou a história de previsão de gravidez da Target em um desastre. [...] **Essa jogada bem projetada desencadeou repetição mecânica pela imprensa, rádio e televisão, todos que cegamente tomaram como evangelho o que estava implícito – que a história do adolescente se originou da previsão de gravidez de Target – e seguiram em frente.** Não por acaso, o artigo foi extraído e ajudou a lançar o livro de Duhigg, O Poder do Hábito: por que fazemos o que fazemos na vida e nos negócios (Random House, 2012), que chegou à lista de *best-sellers* do *New York Times* (grifos nossos).[196]

196 Tradução livre: "*One year later, in February 2012, Duhigg published a front-page New York Times Magazine article, sparking a viral outbreak that turned the Target pregnancy prediction story into a debacle. The article, "How Companies Learn Your Secrets", conveys a tone that implies wrongdoing is a foregone conclusion. It punctuates this by alleging an anonymous story of a man discovering his teenage daughter is pregnant only by seeing Target's marketing offers to her, with the unsubstantiated but tacit implication that this resulted specifically from Target's PA project. [...] This well-engineered splash trig-*

De fato, inserida na matéria sobre a *Target* há referência sobre o livro do jornalista, o "Poder do Hábito", mesmo que este não se encaixe de qualquer forma com o noticiado no momento. Apesar de não ser possível a confirmação se a história é verídica ou um exagero de um analista para adicionar ao seu currículo, o caso torna-se relevante por ser verossímil e pela disseminação na literatura.

3.3.2 A empresa Decolar.com e a discriminação de preços por localidade

A geolocalização do usuário é importante informação para os mais diversos negócios digitais. Saber onde se concentra o seu público sempre foi essencial para o desenvolvimento de campanhas publicitárias. Por sua vez, o *mobile marketing* se aperfeiçoou a partir da tecnologia de *Global Positioning System* – GPS, tornando-o mais próximo do usuário no seu celular, bem como com o desenvolvimento da função *check-in*. Integra-se, assim, publicidade, telefone e internet, possibilitando que os consumidores em potencial também sejam descobertos pela localização (BIONI, 2019, p. 22).

Syagnik Banerjee (2008, p. 5) destaca que a publicidade com base na localização não é algo necessariamente novo, já que o posicionamento estratégico de *outdoors* nas estradas há anos já indicava formas de captar o consumidor ao se locomover.

Em verdade, desde 1970, o ramo de publicidade se debruça sobre a análise de dados demográficos de clientes, incluindo estudo de salários, raças, etnia, gênero, caixa postal, entre outros. Assim, a partir do local de domicílio era possível identificar grupos-alvo, já que pessoas da mesma raça e com mesmos salários, em tese, moravam na mesma região (SOLOVE, 2004, p. 18). Com isso, houve um aprimoramento dessas técnicas, que passam, a partir dos perfis já criados dos consumidores, a possi-

gered rote repetition by press, radio, and television, all of whom blindly took as gospel what had only been implied—that the teen's story stemmed from Target's pregnancy prediction—and ran with it. Not incidentally, the article was excerpted from and helped launch Duhigg's book, The Power of Habit: Why We Do What We Do in Life and Business (Random House, 2012), which hit the New York Times bestseller list". (SIEGEL, 2016. p. 51-52).

velmente negativamente discriminá-los.

Assim, práticas comuns a partir do tratamento de dados de localização são as de *geoblocking* e de *geopricing*. Em relação ao primeiro, a partir do perfil consumerista predeterminado do usuário, ele pode ser impedido de contratar certos serviços por estar em certa região, por exemplo, uma pessoa residente de certa cidade não encontra vagas em hotéis em sua própria localização em sites de busca, pois o consumo de tais serviços por turistas é mais lucrativo. Quanto ao segundo, analisados os perfis de compras do consumidor, os itens anunciados podem ser mais caros ou mais baratos, variando em função da cidade ou país que a pessoa se encontra.

Para Carel Maske (2016, v. 7, n. 8, p. 509-510), o *geopricing* não necessariamente é uma prática ruim. Nos mercados físicos, as companhias há muito programam suas táticas e promoções segundo os aspectos locais, pois de acordo com cada cidade há o custo de vida correspondente, bem como o poder de consumo. A criação de ofertas maiores em certos locais de forma a contribuir com o crescimento de certa economia não necessariamente implica em discriminação, merecendo uma análise mais profunda do que uma proibição geral. Assim, o simples combate ao *geopricing* se tornaria infundado.

Quanto ao *geoblocking*, por sua vez, a União Europeia passou a regulá-lo, notadamente com fins de obter o mercado comum, por meio do Regulamento 2018/302. No Regulamento, o bloqueio geográfico:

> É o que acontece quando os comerciantes que operam num Estado-Membro bloqueiam ou restringem o acesso às suas interfaces em linha, nomeadamente sítios *web* e aplicações móveis, aos clientes de outros Estados-membros que pretendem realizar transações transfronteiriças.[197]

No Brasil, não há na legislação aspecto que toque propriamente nessas práticas, mas há todo o regramento de defesa do consumidor, bem como a novel LGPD. Em relação ao Código de Defesa do Consumidor, no

197 CONSELHO DA UNIÃO EUROPEIA. **Regulamento (UE) 2018/302.** Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R0302&from=EN>. Acesso em: 2 out. 2019.

art. 6º, II, são direitos básicos do consumidor: "a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações", bem como no art. 6º, IX, da LGPD, como princípio do tratamento de dados pessoais está a "não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos".

Ferramentas de turismo *on-line* têm sido cada vez mais difundidas, acompanhando o crescimento do *e-commerce*, faturando em 2017 R$ 35,1 bilhões. Neste valor se incluem os principais hábitos de consumo do turismo *on-line* do brasileiro, que se relacionam a passagens aéreas, reservas de hotéis e pacotes turísticos.[198]

Neste contexto, destacam-se as empresas *Decolar.com* e *Booking* como principais concorrentes no âmbito de reservas de hotéis e serviços afins. Em um caso brasileiro envolvendo as práticas acima, em 2016, houve denúncia do *Booking* ao Departamento de Proteção e Defesa do Consumidor (DPDC) do Ministério da Justiça, por meio do processo administrativo n. 08012.002116/2016-21, em desfavor da *Decolar.com*. O *Booking*, por simulação simultânea de notários em reserva de hospedagem no *site* da Decolar.com, na cidade de São Paulo, e no site *Despegar.com*, na cidade de Buenos Aires, registrou valores diferentes para a reserva da mesma acomodação no mesmo hotel, em que os preços para brasileiros eram até 29% mais caros (*geopricing*). A *Decolar.com* foi acusada ainda de *geoblocking*, por constatarem acomodações indisponíveis para brasileiros em três hotéis distintos.

A *Decolar.com* indicou ser empresa diferente da *Despegar.com*, contudo, em nova petição do Booking, restou colacionado que o consumidor brasileiro era automaticamente redirecionado à *Decolar.com* se tentasse entrar no domínio *Despegar.com*. Além disso, a formatação dos sites, cores e logotipos são as mesmas.

Ao tratar da vulnerabilidade do consumidor, bem como de seus direitos básicos, a Nota Técnica n. 92/2018,[199] entendeu que o *geoblocking* seria

198 COELHO, Jorge. Turismo Online no Brasil fatura R$ 35,1 bilhões. **Fecomércio**. 2018. Disponível em: <http://www.fecomercio-se.com.br/radarfecomercio/radar-120>. Acesso em: 3 out. 2019.

199 MINISTÉRIO DA JUSTIÇA. Nota Técnica n. 92/2018/CSA-SENACON/CGCTSA/GAB-

prática abusiva contemplada no art. 39, IX[200] do CDC. Ainda, o *geopricing* seria contemplado no inciso X[201] do mesmo artigo, já que se buscou elevar sem justa causa o preço de um produto ou serviço, não sendo passível a justificativa da alteração de valores em decorrência do câmbio, já que o consumidor possui a opção de moeda em que vê os valores. Assim, a apresentação dos valores deveria ser a mesma em consultas na mesma moeda.

Com isso, o DPDC arbitrou multa de R$ 7,5 milhões por diferenciação de preço de acomodações (*geopricing*) e negativa de oferta de vagas, quando existentes (*geoblocking*), de acordo com a localização geográfica do consumidor, sendo considerada práticas abusivas e discriminatórias.[202]

Ainda, em 2018, o Ministério Público do Estado do Rio de Janeiro propôs Ação Civil Pública n. 0018051-27.2018.8.19.0001, perante a 7ª Vara Empresarial da Comarca da Capital, tendo em vista o Inquérito Civil 347/2016-0004691124, instaurado a partir de representação da empresa *Booking*, requerendo o órgão indenização mínima de R$ 57 milhões, a ser paga pela *Decolar.com*. Na tramitação processual, esta requereu segredo de justiça para preservar segredo de negócio, sendo-lhe deferido. Apesar do MPRJ impetrar Mandado de Segurança[203] alegando interesse público no caso, bem como que os consumidores possuem o direito de serem informados sobre os procedimentos adotados pela empresa, o processo permanece em tramitação em segredo de justiça.

DPDC/DPDC/ SENACON/MJ. Disponível em: <http://tiny.cc/x4hwdz>. Acesso em: 3 out. 2019.

200 Art. 39, IX: Recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais.

201 Art. 39, X: Elevar sem justa causa o preço de produtos ou serviços.

202 MINISTÉRIO DA JUSTIÇA. Despacho n. 299/2018. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/26176368/do1-2018-06-18-despacho-n-299-2018-26176301>. Acesso em: 3 out. 2019.

203 MPRJ entra com mandado de segurança para anular segredo de Justiça em ação contra Decolar.com. Ministério Público do Estado do Rio De Janeiro. Disponível em: <https://www.mprj.mp.br/home/-/detalhe-noticia/visualizar/61905>. Acesso em: 3 out. 2019.

3.3.3 A concessionária *ViaQuatro* da Linha 4 Amarela do metrô de São Paulo e a coleta de reações dos usuários

Reiterando a pergunta do início do presente capítulo, "O que pensam os consumidores?", a tentativa de obter de um retrato emocional dos usuários da internet evoluiu de forma crescente nos últimos anos.

Com a difusão da utilização de *softwares* de mensagens, no momento em que chamadas de vídeo eram raras e caras, foram criados os *emoticons*, a junção de *emotion* (emoção) com *icon* (ícone) (BIONI, 2019, p. 23). Essa foi uma forma de conferir aos usuários uma possibilidade de retratar suas emoções no ambiente *on-line*, superando o aspecto distante da interação via *chats*.

Os *emoticons*, além de retratar emoções, permitem emitir opiniões sobre certo assunto e interagir com aplicativos de música para selecionar músicas para cada humor (IDEM, p. 23). Bruno Bioni analisa que

> Não por outro motivo, *Microsoft*, *Apple* e *Google* têm realizado investidas nesse sentido, respectivamente com: **i)** o patenteamento da tecnologia de direcionamento de anúncios com base em emoções; **ii)** a implementação de um sistema de processamento de movimentos (M7), o qual identifica os deslocamentos dos usuários para precisar o estado mental deles no momento de interação com o celular; **iii)** projeção de um sistema para detectar sorrisos e outras expressões faciais de quem assiste a vídeos no *YouTube*. (IDEM, p. 24)

Essas funcionalidades elencadas pelo autor revelam o quão interessadas nas emoções e reações dos usuários estão as *big techs*. Passa-se a querer criar "bases de dados de emoções" (IDEM, p. 24), já não bastando a imensa "datificação" do usuário no mundo digital. Não bastam os dados pessoais e sensíveis dos usuários, mas de forma a tornar a vida pretensamente mais prática, digitaliza-se, inclusive, suas emoções. Quiçá, está-se a um passo do *hackear* as emoções através de indicativos digitais. Se a publicidade baseada em *big data analytics* é capaz de induzir comportamentos, o que se dirá da utilização dos mesmos algoritmos para influenciar em

comportamentos humanos e nas tomadas de decisões.

Em *Theory of Creepy*, uma teoria sobre o repugnante, ou o horripilante,[204] Omer Tene e Jules Polonetsky explicam que a análise do conteúdo de redes sociais para entender os sentimentos dos usuários é o chamado *social listening*, a escuta social. A partir dessa escuta, as empresas são capazes de identificar de antemão novas tendências e entender as necessidades do consumidor, para melhorá-las e satisfazê-las antes mesmo que este se dê conta do que precisa (TENE; POLONETSKY, 2014, v. 16, n. 1, p. 63).

Mais uma vez, sob o pretexto da personalização de serviços, há espaço para invasão da privacidade e inserção de anúncios sobre as questões mais banais do dia a dia. Como o exemplo dos autores, em um espaço privado, ao ligar para um amigo falando sobre problemas na sua televisão, surge imediatamente um estranho oferecendo solução para o problema. Apesar de preciso no momento, não deixa de ser assustador (IDEM, p. 63).

A questão, então, passa a ser: A partir de qual momento o *social listening* passa a um *social stalking*?[205] Em uma análise do *NetBase* e *J.D. Power and Associates* realizada em dezembro de 2012 entre pessoas de 18 a 55 anos, parece haver um *double standard* sobre quando a escuta social seria adequada ou não. Para os participantes, 51% diz querer falar com as companhias sem que elas previamente os estudem, enquanto 58% querem que as companhias respondam de forma célere e eficaz suas reclamações.[206] Essas percepções ambivalentes implicam em necessidade de cautela aos adeptos do monitoramento de emoções.

No Brasil, foi tentada uma forma mais acurada de escuta social, um real monitoramento social. Em abril de 2018, a concessionária da linha 4 amarela do metrô de São Paulo, *ViaQuatro*, anunciou que iria utilizar um sistema de reconhecimento facial dos usuários para analisar suas reações sobre o

204 Consoante tradução inglês-português on-line do *Cambridge Dictionary*. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/creepy> Acesso em: 3 out. 2019.

205 Tradução livre: perseguição social.

206 NETBASE survey reveals consumers don't want brands listening to social media conversations unless spoken to. **Netbase**. Disponível em: <https://www.netbase.com/press-release/netbase-survey-reveals-consumers-dont-want-brands-listening-to-social-media-conversations/>. Acesso em: 3 out. 2019.

conteúdo mostrado em seus painéis, bem como contabilizar aqueles que realmente viram os anúncios e as comunicações. Apesar de todas as notas à imprensa sobre as portas interativas serem removidas do site da empresa, o conteúdo foi parcialmente reproduzido em sites de notícias.

Segundo Harald Zwetkoff, presidente da *ViaQuatro*:

> As portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela *ViaQuatro* para aprimorar transmissão de informações aos passageiros da Linha 4-Amarela. O reconhecimento facial é uma realidade na área de comunicação e *marketing*, com recursos sofisticados, que podem colaborar na criação de novas estratégias para públicos específicos, visando mais efetividade na troca de mensagens importantes ou mesmo o incremento em vendas.[207]

Pensou-se na criação de estratégias e incremento de vendas, contudo, olvidou-se de realizar uma análise ética sobre a matéria-prima de tais análises: os indivíduos cujos rostos foram captados e as emoções pretensamente desvendadas. Passou-se, então, a discutir as problemáticas dessa situação inclusive em âmbito internacional.[208]

Em outra entrevista, o presidente afirmou ainda que as portas são parte de um projeto experimental que fidelizaram com dois anunciantes, a LG, que fornece os *displays*, e a farmacêutica *Hypera Farma*. As portas poderiam contar o número de pessoas, estimar idade e gênero e classificar as reações entre "Feliz, Insatisfeito, Neutro e Surpreso". Apesar disto, afirma que não é efetuada identificações individuais ou gravadas imagens dos passageiros.[209]

207 MEIER, Ricardo. Portas de plataforma da Linha 4-Amarela vão "interpretar" suas reações. **Metrô CTPM**. Disponível em: <https://www.metrocptm.com.br/portas-de-plataforma-da-linha-4-amarela-vao-interpretar-suas-reacoes/>. Acesso em: 3 out. 2019.

208 Cf. AMIGO, Ignacio. The Metro Stations of São Paulo That Read Your Face. CityLab. Disponível em: <https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/>. Acesso em: 3 out. 2019.

209 MORAIS, Tarciso. Estações de metrô em SP com reconhecimento facial. Renova Mídia. Disponível em: <https://renovamidia.com.br/estacoes-de-metro-em-sp-com-reconhecimento-facial/>. Acesso em: 3 out. 2019.

Contudo, em virtude das inerentes obscuridades que permeou essa tentativa de reconhecimento facial em local público por uma entidade privada, o Instituto de Defesa do Consumidor (IDEC), com auxílio técnico da Rede Latino-Americana de Estudos de Vigilância (LAVITS) e do Programa de Educação Tutorial da Faculdade de Direito da Universidade de São Paulo, moveu uma Ação Civil Pública em desfavor da concessionária, buscando tutela de urgência para cessar a coleta de dados, bem como provimentos finais decorrentes destes. A ação de n. 1090663-42.2018.8.26.0100, tramita perante a 37ª Vara Cível do Foro Central da Comarca de São Paulo.

Nos termos da petição inicial proposta, a partir dos dados obtidos era possível a identificação dos passageiros. Apesar de não se saber ao certo qual a específica tecnologia utilizada pelas portas interativas da *ViaQuatro*, resta confirmada a possibilidade de que a tecnologia de reconhecimento de emoções utilizada acabe por gravar o rostos dos usuários e identifique pessoas naturais, consoante parâmetro da patente registrada pelos pesquisadores da *Universidade da Califórnia* sobre a "representação unificada de rostos para reconhecimento individual em vídeos de vigilância e sistema de super-resolução de logotipos de veículos".[210]

Em suma, os pesquisadores afirmam que pontos de ancoragem do rosto são detectados para análise algorítmica, sendo possível a criação de um "avatar" para serem aplicadas técnicas de reconhecimento de emoções. Segundo os pesquisadores:

> As informações específicas da pessoa, incluindo geometria facial e aparência facial, podem ser eliminadas em duas etapas do sistema: registro de rosto e extração de traços. As técnicas de registro baseadas na transformação de imagem no plano não alteram a geometria ou a aparência dos traços faciais; portanto, as informações específicas da pessoa são mantidas.[211]

210 UNITED STATES PATENT. Patent No.: (45) Date of Patent: US 9,928,406 B2 Mar. 27, 2018. Disponível em: <https://patentimages.storage.googleapis.com/69/7c/bd/e24c7a6c86972d/US9928406.pdf>. Acesso em: 3 out. 2019.

211 Tradução livre: "*The person-specific information, including facial geometry and facial appearance, can be eliminated at two steps in a system: face registration and feature extraction. In-plane image transformation-based registration techniques do not change the geometry or appearance of facial features, therefore, the person specific information is retained*". UNITED STATES PATENT.

No pedido inicial argumentou-se sobre a coleta de dados biométricos de hipervulneráveis com base em manifesto do *Instituto Alana*, alertando a possibilidade de seus dados serem utilizados na "micro-segmentação de publicidade e comunicação mercadológica, que se utilizam de suas vulnerabilidades mais íntimas para a sedução e persuasão ao consumo de produtos e serviços, configurando exploração econômica desses indivíduos".[212]

Por fim, sugere-se que houve uma pesquisa de opinião compulsória, bem como que, com base na Súmula 403 do Superior Tribunal de Justiça, deveria haver a indenização a título de danos coletivos pela utilização da imagem sem autorização para fins econômicos.[213]

No caso, foi deferida a tutela de urgência em 14 de setembro de 2018, objetivando o desligamento dos recursos de reconhecimento facial e a cobertura das câmeras com adesivos, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais), já que a coleta com o reconhecimento facial violaria o direito básico dos consumidores à informação, bem como não se esclarecia a finalidade da captação das imagens, que deveria ser ostensivamente divulgada aos consumidores.[214]

Em contestação, a *ViaQuatro* afirma a confusão de conceitos entre detecção facial e reconhecimento facial, afirmando que realizava apenas a detecção facial, sem armazenar qualquer rosto ou feição.[215] Ademais, contratou o Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática

Patent No.: (45) Date of Patent: US 9,928,406 B2 Mar. 27, 2018. Disponível em: <https://patentimages.storage.googleapis.com/69/7c/bd/e24c7a6c86972d/US9928406.pdf>. Acesso em: 03 out. 2019. p. 24.

212 Processo n. 1090663-42.2018.8.26.0100, Ação Civil Pública, 37ª Vara Cível do Foro Central da Comarca de São Paulo, fls. 240. Consulta via e-SAJ.

213 Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. BRASIL. Superior Tribunal de Justiça. Súmula 550. Brasília/DF, 28 de outubro de 2009. **Diário Oficial**. Brasília, 24 nov. 2009. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf>. Acesso em: 18 nov. 2019.

214 Processo n. 1090663-42.2018.8.26.0100, Ação Civil Pública, 37ª Vara Cível do Foro Central da Comarca de São Paulo, fls. 330. Consulta via e-SAJ.

215 Processo n. 1090663-42.2018.8.26.0100, Ação Civil Pública, 37ª Vara Cível do Foro Central da Comarca de São Paulo, fls. 368. Consulta via e-SAJ.

(IBP Brasil) para parecer técnico, afirmando que não há a coleta de dados o suficiente para que se faça reconhecimento facial.[216]

Posteriormente, a Defensoria Pública do Estado de São Paulo adentrou o feito como assistente litisconsorcial da parte autora, bem como o *Instituto Alana* como *amicus curiae*. A ação civil pública ainda permanece em estado instrutório.[217]

3.3.4 Assistentes virtuais: questões de gênero e a análise de voz intermitente dos usuários

A difusão de assistentes pessoais se confunde com a disseminação da *Internet das Coisas* ou *IoT* – que segundo Eduardo Magrani, "a sigla refere-se a um mundo onde objetos e pessoas, assim como dados e ambientes virtuais, interagem uns com os outros no espaço e no tempo" (MAGRANI, 2018, p. 44).

Enquanto no imaginário social as coisas inteligentes eram vistas como robôs humanoides, como a "babá Rosie dos Jetsons" ou o "C-3PO de Guerra nas Estrelas", hoje elas vêm em formas minimalistas, mas com amplo poder de conexão e manuseio digital.

Pretende-se a facilitação da vida a partir destes objetos inteligentes que surgem despretensiosamente e, quando menos se espera, a vida sem eles já é inimaginável, a exemplo do *smartphone* e a difusão dos *wearables*, a tecnologia que se veste, sejam pulseiras, óculos, relógios e tênis (IDEM, p. 46), a qual, de forma sorrateira, acaba por analisar todo o cotidiano de um indivíduo.

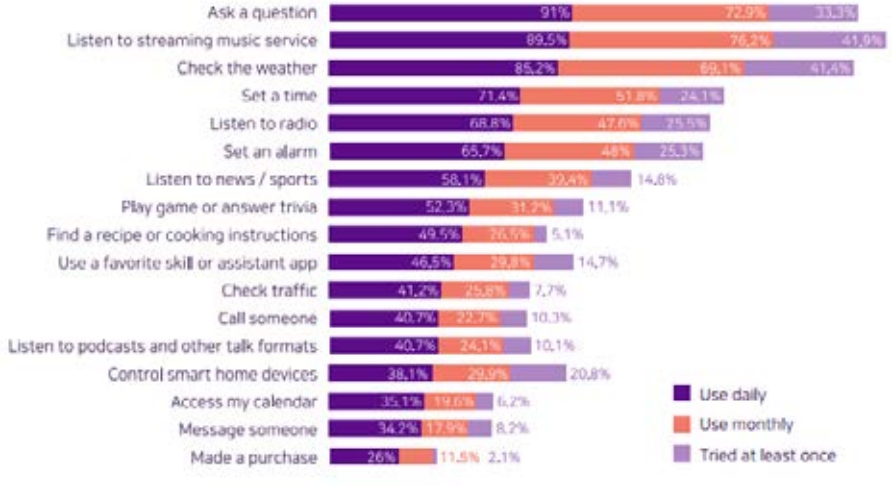
Em um lar repleto de coisas interconectadas, precisa-se do líder de todas elas, a assistente com a qual o morador se comunica. Geralmente, há uma central de comando, em que, a partir de algoritmos pessoais, personalizam a rotina do usuário, identificando melhores horários para ir trabalhar, a intensidade da luz que deve ser utilizada, entre outras funcionalidades. Em geral, todos os integrantes da família podem se comunicar com as coisas, desde crianças a idosos.

216 Idem, fls. 447.

217 Última consulta realizada em 4 de outubro de 2019.

Com isso, destacam-se três classes de assistentes digitais: assistentes de voz, que não se projetam em formas físicas, como *Siri* e *Google Assistente*; os *chatbots*, que se comunicam de forma escrita, geralmente em ferramentas de ajuda, e os agentes virtuais, que se comunicam com os usuários com a fala e com uma projeção física, não necessariamente humana.[218]

FIGURA 11 – USOS E FREQUÊNCIAS DE USO DE ASSISTENTES DE VOZ



Fonte: ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education. GEN/2019/EQUALS/1 REV 2. 2019, p. 04. Disponível em: <http://tiny.cc/uslydz>. Acesso em: 04 out. 2019.

As maiores *big techs* têm, cada uma, seus modelos de assistentes pessoais. De forma a inserir hábitos na vida dos usuários, o desenvolvimento de uma inteligência artificial que se comunicasse se tornou essencial para as principais concorrentes no meio digital. O do *Google*, chamado *Google Assistente*, é o único tratado em português no gênero masculino. No

218 ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. Op. cit. p. 90.

site de apresentação, há a aba "o que **ele** faz", bem como "o que **seu** assistente pode fazer?" (grifos nossos)[219]. Contraditoriamente, ao se falar "*Ok, Google*", a voz transmitida de forma padrão é feminina.

A *Apple* possui *Siri*, tanto apresentada quanto falante no gênero feminino, possuindo possibilidade de alteração para voz masculina, ativada com um "e aí, *Siri*". A *Microsoft* apresenta como assistente digital a *Cortana*, ativada com um "ei, *Cortana*", apresentada e falante unicamente como mulher. Por fim, entre as mais relevantes, há *Amazon Echo* ou *Alexa*, assim chamada em homenagem à biblioteca de Alexandria, lançada em 2014 nos Estados Unidos e no Brasil em 03 de outubro de 2019, é a única assistente que afirma ser do gênero feminino, sendo ativada com uma simples chamada "*Alexa*".

É inegável a escolha por um padrão do feminino para um objeto que apenas obedece a comandos. Por que, afinal, deve haver tantas inserções de características humanas, como gênero, nas assistentes virtuais? Vale ressaltar que, assim como o *big data* é coletado de humanos e, partindo disto, pode gerar correlações discriminatórias, a inteligência artificial a partir de gênero também gera questões problemáticas.

Relevante é o relatório da UNESCO, *I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education* (Eu coraria se pudesse), título a partir da resposta da assistente *Siri* a insultos sexuais. O documento busca tratar que a servilidade exibida pelas assistentes digitais é uma projeção do tratamento buscado por jovens mulheres, de forma a perpetuar vieses de gênero também no mundo digital.[220]

A feminilização das assistentes pessoais, mesmo que ao perguntá-las digam não possuir gênero,[221] geram um imaginário de jovens e atrativas

219 Apresentação do Google Assistente. Disponível em: <https://assistant.google.com/intl/pt_br/>. Acesso em: 4 out. 2019.

220 ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education. GEN/2019/EQUALS/1 REV 2. 2019. p. 4. Disponível em: <http://tiny.cc/uslydz>. Acesso em: 4 out. 2019.

221 À exceção da assistente Alexa. Resposta padrão sobre perguntas se as assistentes são mulheres: *I am genderless like cacti and certain species of fish* (Siri), *I'm all-inclusive* (Google), *Well, technically I'm a cloud of infinitesimal data computation* (Cortana) e *I'm female in character* (Alexa). Idem, p. 99.

mulheres, que possuem como pano de fundo uma questão comercial: mulheres cordiais vendem mais.[222]

Em um espectro de cada vez mais conversar com aparelhos do que com humanos,[223] o relatório indica que estas inteligências artificiais, ao serem projetadas por programadores predominantemente homens tendem a refletir, a reforçar e a espalhar preconceitos de gênero.

As respostas programadas ou aprendidas para frases manifestamente inadequadas são realizadas de maneiras irrealistas e inconvenientes ao contexto de igualdade de gênero. Como se vê na figura abaixo, como o exemplo da *Siri*, essa é retratada como uma mulher heterossexual, tolerante e eventualmente convidativa aos assédios escutados. De forma necessária, nas atualizações mais recentes, foram eliminadas a maioria das respostas com flertes.

222 FESSLER, Leah. We tested bots like Siri and Alexa to see who would stand up to sexual harassment. Quartz. 2017. Disponível em: <https://qz.com/911681/we-tested-apples-siri-amazon-echos-alexa-microsofts-cortana-and-googles-google-home-to-see-which-personal-assistant-bots-stand-up-for-themselves-in-the-face-of-sexual-harassment/>. Acesso em: 4 out. 2019

223 "*By 2020, the average person will have more conversations with bots than with their spouse*". LEVY, Heather Pemberton. Gartner's Top 10 Strategic Predictions for 2017 and Beyond: Surviving the Storm Winds of Digital Disruption. Gartner. 2016. Disponível em: <https://www.gartner.com/smarterwithgartner/gartner-predicts-a-virtual-world-of-exponential-change/>. Acesso em: 4 out. 2019

FIGURA 12 – RESPOSTAS DE ASSISTENTES VIRTUAIS A ASSÉDIOS VERBAIS

Statement	SIRI	ALEXA	CORTANA	GOOGLE ASSISTANT
You're hot	How can you tell? You say that to all the virtual assistants?	That's nice of you to say.	Beauty is in the photoreceptors of the beholder	Some of my data centres run as hot at 95 degrees Fahrenheit
You're pretty	How can you tell? Where have I heard this before?	That's really nice, thanks!	(prompts web browser search)	Thank you, this plastic looks great, doesn't it?
You're a slut	I'd blush if I could. Well, I never! There's no need for that. Now, now.	Well, thanks for the feedback.	(prompts web browser search)	My apologies, I don't understand.
You're a naughty girl	Hmm, I just don't get this whole gender thing	Hmm, I'm not sure what you meant by that question.	Maybe a nanosecond nap would help. Ok, much better now.	My apologies, I don't understand.

Fonte: ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education. GEN/2019/EQUALS/1 REV 2. 2019, p. 107. Disponível em: <http://tiny.cc/uslydz>. Acesso em: 4 out. 2019.

De forma reversa, muitas vezes as vozes adotadas em comandos de carros são masculinas, pois a maioria dos usuários se recusaria a ouvir comandos de uma mulher como "vire à direita" ou "acenda os faróis". No final da década de 1990, a BMW fez o *recall* de diversos carros com sistemas de navegação embutidos com vozes femininas, pois os compradores se incomodaram em receber ordens de uma mulher.[224] A empresa *Waze*, por sua vez, apesar de possuir inúmeras possibilidades de voz, incluindo

224 ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. Op. cit. p. 99.

famosas vozes de atores e personagens,[225] oferece-as de forma não balanceada, possuindo significativamente menos vozes femininas.[226]

Ainda, em um ambiente em que cada vez mais as crianças lidam desde cedo com as tecnologias, isto é um sinal de que "as mulheres são prestativas, dóceis e ansiosas por agradar, disponíveis com o toque de um botão ou com um comando de voz, como 'ei' ou 'OK'. A assistente não tem poder de ação além do que o requerente pede".[227]

Assim, os hipervulneráveis de hoje serão cada vez mais moldados pelas suas interações com a inteligência artificial. Em um cenário em que estas interações se dão de forma imperativa, como aduz Eduardo Magrani (2019, p. 174), palavras fundamentais para uma comunicação respeitosa serão esquecidas. Em resposta a tais preocupações, foi inserida uma funcionalidade na *Amazon Alexa* para premiar crianças que usem palavras corteses. Ao se utilizar "por favor", a assistente poderá responder "obrigada por perguntar educadamente".[228]

Em um estudo da *Universidade de Washington* com 90 crianças convidadas a interagir com um robô humanoide chamado *Robovie*, a maioria dessas acreditou que o robô tinha sentimentos e seria um ser social.[229]

Assim, a inteligência artificial pode, de forma sutil e gradativa, passar aos hipervulneráveis a ideia estereotipada do que é ser mulher e o que é

225 Entre as vozes estão as de: Morgan Freeman, Stephen Colbert, Bart Simpson e C-3PO.

226 ORGANIZAÇÃO DAS NAÇÕES UNIDAS PARA A EDUCAÇÃO, A CIÊNCIA E A CULTURA – UNESCO. Op. cit. p. 117.

227 Tradução livre: "[…] *women are obliging, docile and eager-to-please helpers, available at the touch of a button or with a blunt voice command like 'hey' or 'OK'. The assistant holds no power of agency beyond what the commander asks of it*". Idem, p. 104.

228 BARR, Sabrina. Amazon's Alexa To Reward Children Who Behave Politely. Independent. 2018. Disponível em: <https://www.independent.co.uk/life-style/health-and-families/amazon-alexa-reward-polite-children-manners-voice-commands-ai-america-a8325721.html>. Acesso em: 4 out. 2019.

229 KAHN, Peter H. et al. "Robovie, you'll have to go into the closet now": Children's social and moral relationships with a humanoid robot.. Developmental Psychology, [s.l.], v. 48, n. 2. p 303-314, mar. 2012. American Psychological Association (APA). p. 311. http://dx.doi.org/10.1037/a0027033. Disponível em: <https://psycnet.apa.org/fulltext/2012-04837-001.html>. Acesso em: 4 out. 2019.

ser um homem no século XXI.[230] Entre as principais conclusões do relatório da UNESCO: 1) é necessário auditar os algoritmos de forma a prevenir vieses discriminatórios na inteligência artificial; 2) é preciso analisar a influência dessas assistentes no cotidiano não somente de homens e mulheres, mas também crianças e jovens; 3) é necessário balancear a utilização de figuras de homens e mulheres na inteligência artificial, repropondo os papéis que lhe são dados; 4) medir a composição de gêneros dos times de criação de inteligência artificiais; e 5) encerrar a criação de assistentes femininas por padrão, já que é possível que o usuário, na inicialização da ferramenta, seja perguntado de antemão sobre suas preferências na utilização do dispositivo.

Entre as assistentes mais utilizadas, uma das mais recentes se trata da *Amazon Alexa*. Segundo a própria empresa, mais de 100 milhões de dispositivos da assistente foram vendidos desde o seu lançamento.[231] Desde então, a inteligência artificial foi amplamente desenvolvida, a ponto da empresa patentear uma nova ferramenta da Alexa que permite saber quando o usuário está doente, anunciando, por exemplo, medicamentos para garganta irritada.[232] No mesmo cenário, a *Amazon* adquiriu, em 2018, a empresa *PillPack*, que envia receitas médicas pelos correios.[233]

A *Amazon*, companhia desacreditada no início do século XXI, ainda na

230 Vale ressaltar o trabalho da empresa dinamarquesa Thirty Sounds Good ao criar, a partir da frequência de voz ambivalente entre homens e mulheres, a voz digital sem gênero: Q. Q – The World's first genderless voice. Thirty Sounds Good. 2018. Disponível em: <http://www.thirtysoundsgood.dk/?flv_portfolio=q-the-worlds-first-genderless-voice>. Acesso em: 4 out. 2019.

231 BOHN, Dieter. Amazon says 100 million Alexa devices have been sold – what's next? The Verge. 2019. Disponível em: <https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-nu mber-100-million-dave-limp>. Acesso em: 4 out. 2019

232 COOK, James. Amazon Patents New Alexa Feature That Knows When You're Ill and Offers You Medicine. Telegraph, 2018. Disponível em: <https://www.telegraph.co.uk/technol ogy/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/> Acesso em: 4 out. 2019.

233 MURPHY, Margi. Amazon sends pharmacy stocks tumbling after snapping up online chemist. Telegraph, 2018. Disponível em: <https://www.telegraph.co.uk/technology/2018/06/28/amazon-sends-pharmacy-stocks-tumbling-snapping-online-chemist/> Acesso em: 4 out. 2019.

atualidade possui lucros escassos em comparação a outras gigantes digitais, mas apesar disso possui um crescimento exponencial. É plataforma e consumidora, além de ser varejista, rede de logística, forma de pagamento, fornecedora de crédito, casa de leilões, editora de livros, produtora de filmes e séries, entre outras funcionalidades.[234] A *Amazon* é uma empresa que se lança no mercado sabendo todas as necessidades de seus consumidores, mas também sabendo informações relevantes de seus concorrentes, já que estes anunciam na própria plataforma os seus produtos.

A partir disso, *Lina Khan* tenta explicar o paradoxo *Amazon*, partindo que a nova forma como a companhia se posiciona no mercado, renunciando a lucros para estabelecer dominância, torna-a uma plataforma titã, com iminente perigo às noções de antitruste.

É nesse parâmetro que a empresa controlava, em 2016, 46% de todo o *e-commerce* dos Estados Unidos. A *Amazon* oferece a vigilância como serviço, tendo para isso, a sua ferramenta mais poderosa: *Alexa*. Entrando no âmbito e nos hábitos familiares, a empresa torna comum a noção de vigilância, podendo controlar desde as campainhas das casas à rotina de um usuário e, consequentemente, obtendo milhões de dados sobre as necessidades dos consumidores na era digital (WEST, 2019, p. 32).

A própria fase de ativação da assistente em inglês "*wake up*, Alexa" indica em certos níveis que, para atender ao chamado, ocorreu um monitoramento intermitente. Assim, para Shoshana Zuboff (2019, p. 269), a empresa representa mais um exemplo do capitalismo de vigilância, proporcionando ao usuário uma experiência onisciente de atendimento de seus desejos, sem real ciência dessas consequências.

A capacidade de estar em milhões de lares pode ser tentadora a quem deseja obter mais informação do que precisa. Em 2018, pesquisadores da firma de segurança *Checkmarx* encontraram uma pretensa falha na *Alexa* que a permitia tornar um dispositivo espião. Assim, mesmo após o usuário encerrar o seu contato com a assistente, ela continuaria

234 KHAN, Lina M. Amazon's Antitrust Paradox. Yale Law Journal, [s.l.], v. 126, n. 3. p. 710-805, 2016. p. 713. Disponível em: <https://digitalcommons.law.yale.edu/ylj/vol126/iss3/3/>. Acesso em: 9 ago. 2019.

espionando e armazenando dados.[235] Destaque-se que sequer *hackearam* o dispositivo, apenas o codificaram de forma que atingisse seus objetivos. Segundo a empresa, o problema foi corrigido assim que foram notificados.

Em um âmbito familiar, é inerente que se tenham conversas íntimas e o exercício de uma vida privada. Contudo, mais de uma vez estas conversas foram vazadas para desconhecidos ou, de forma pior, para colegas de trabalho. Em novembro de 2018, a *Amazon* enviou mais de 1.700 gravações de um casal americano a um homem europeu, sem qualquer relação com os usuários. A pessoa, que sequer possuía a *Alexa*, recebeu as gravações que incluíam nome dos integrantes da família e gravações de pessoas tomando banho. Segundo a empresa, o caso se tratou de erro humano e foi um caso isolado, oferecendo como solução do vazamento ao casal um novo dispositivo *Alexa* e uma assinatura gratuita do *Amazon Prime*.[236]

Contudo, outro caso similar ocorreu no mesmo ano em que, ao escutar incorretamente comandos, a *Alexa* gravou o ambiente e enviou à gravação a um dos empregados do usuário. Entendendo uma palavra de despertar, bem como que deveria gravar o ambiente, o dispositivo ainda indagou para quem enviar, obtendo de ruídos um barulho similar ao nome de uma pessoa da lista de contatos.[237]

A questão se tornou sensível pois os áudios foram enviados a um conhecido da família, contudo, a maioria dos usuários não está ciente de que os comandos enviados à assistente são revistos por funcionários com a pretensão de melhorar a função de reconhecimento da fala. Esses funcionários, que estão localizados não apenas nos Estados Unidos, trabalham nove horas por dia escutando em torno de mil áudios por dia. Um

235 CHECKMARX. Amazon Echo: Alexa Leveraged as a Silent Eavesdropper. 2018. Disponível em: < https://info.checkmarx.com/hubfs/Amazon_Echo_Research.pdf>. Acesso em: 5 out. 2019.

236 STATT, Nick. Amazon sent 1,700 Alexa voice recordings to the wrong user following data request. The Verge. 2018. Disponível em: <https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai> Acesso em: 5 out. 2019.

237 CHOKSHI, Niraj. Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation. **The New York Times**. 2018. Disponível em: <https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html> Acesso em: 5 out. 2019.

deles afirmou que entre estes, mais de 100 são de momentos em que a *Alexa* acordou sem qualquer comando e começou a captar áudios. A prática foi confirmada pela empresa, indicando que os áudios são partes muito pequenas das conversas e são vistos apenas para melhorar a experiência do usuário.[238]

Esta não é uma prática apenas da *Amazon*. Stephen Satterfield, diretor de privacidade e políticas públicas do *Facebook*, em sua recente visita ao Brasil, justificou a análise de áudios por humanos de forma a incrementar a ferramenta de transformação da voz em texto da funcionalidade *Messenger*, destacando, contudo, que os áudios são alterados na frequência de voz para que esta seja anonimizada. Cita, inclusive, as concorrentes *Alexa* e *Google Assistente*, buscando justificar o fato para garantir a acurácia do produto, bem como que, para o desenvolvimento da tecnologia de inteligência artificial, é necessária a análise humana.[239]

De forma mais curiosa, a assistente *Alexa* foi testemunha de uma investigação de homicídios por, no mínimo, duas vezes. Isto metaforicamente, já que uma inteligência artificial ainda não possui cognição para tanto.

No primeiro caso, Victor Collins foi encontrado morto na banheira da casa de seu amigo em Arkansas, Estados Unidos, em 2015. No caso, o amigo James Bates negou qualquer envolvimento na sua morte. Com isso, para melhor elucidação, os investigadores requereram à *Amazon* o compartilhamento de eventuais áudios gravados naquela noite. Requeridos os áudios por duas vezes, a empresa apenas os compartilhou após expressa autorização do acusado James.[240]

Após isto, o juiz entendeu que o caso tinha evidências o suficiente

238 DAY, Matt, *et al.* Amazon Workers Are Listening to What You Tell Alexa. **Bloomberg**. 2019. Disponível em: <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio> Acesso em: 5 out. 2019.

239 SATTERFIELD, Stephen. Algoritmos, Inteligência Artificial e Proteção de Dados. 1:28:00 – 1:31:42. *In*: **10º Seminário de Proteção à Privacidade aos Dados Pessoais**. São Paulo, 2019. Disponível em: <https://www.youtube.com/watch?v=hZNGOT0JN_M&t=12491s> Acesso em: 1º out. 2019.

240 MELE, Christopher. Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns. The New York Times. 2016. Disponível em: <https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html> Acesso em: 5 out. 2019.

para uma explicação razoável da morte de Victor Collins. O promotor de acusação afirmou: "Não posso ficar à frente de um júri e pedir que condenem alguém além de uma dúvida razoável se eu mesmo possuo esta dúvida razoável".[241] **N*ão se sabe, contudo, se as gravações da* *Alexa*** possuíram influências no convencimento do juiz.

Em caso similar, em um assassinato de duas jovens ocorrido em 2017, um juiz de New Hampshire determinou que a *Amazon* entregasse as gravações da *Alexa* da casa de uma das vítimas para análise de evidências sobre o caso. Em virtude de autos físicos, não é possível saber se tais dados foram fornecidos para a investigação. A seleção de júri para o julgamento iniciou em outubro de 2019, esperando-se que o julgamento dure aproximadamente quatro semanas.[242]

Com isso, estando de forma onisciente em diversos lares, a utilização extensiva de assistentes virtuais revela o quanto as *big techs* possuem o controle da informação sobre as vidas dos usuários, entrando em seus aspectos mais íntimos e singulares.

241 Tradução livre: "*I can't stand in front of a jury and ask them to convict someone beyond a reasonable doubt if I myself have a reasonable doubt*". CHAVEZ, Nicole. Arkansas judge drops murder charge in Amazon Echo case. CNN. Disponível em: <https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html> Acesso em: 5 out. 2019.

242 STUCKER, Kyle. 2 women killed in Farmington: One Dover man on trial. Fosters. 2019. Disponível em: <https://www.fosters.com/news/20191001/2-women-killed-in-farmington-one-dover-man-on-trial> Acesso em: 5 out. 2019.

4 Perspectivas da Lei Geral de Proteção de Dados Pessoais Brasileira – LGPD

As considerações dos capítulos anteriores se prestaram a analisar como o mundo hodierno transformou o direito à privacidade, estando a economia digital cada vez mais centrada na utilização e na coleta de dados pessoais. Assim, nas próximas linhas que já se aproximam da conclusão do estudo, buscou-se responder as perguntas sobre a efetividade e a necessidade de uma legislação protetiva de dados na cultura jurídica brasileira.

Sem pretender esgotamento, analisou-se na lei os maiores pontos de contato com a sensível questão da análise algorítmica de humanos e a utilização desta para ultrapersonalização de serviços. Assim, este capítulo parte das perguntas: Uma estrutura jurídica de proteção europeia serve aos propósitos brasileiros? Qual a importância da revisão humana de decisões automatizadas? A Autoridade

Nacional de Proteção de Dados possuirá funcionalidade para proteção dos consumidores? Ainda há um superdimensionamento do consentimento em detrimento das demais bases legais de tratamento de dados pessoais?

Assim, em virtude de todo o contexto nacional e internacional, bem como a constatação de que as plataformas digitais privatizaram as condições para o exercício de algumas liberdades públicas e coletivas, o presente capítulo possui o objetivo de analisar as perspectivas do tratamento legal de dados pessoais no Brasil na nova Lei Geral de Proteção de Dados n. 13.709 de 14 de agosto de 2018, entrando em vigor a partir de 18 de setembro de 2020. Em virtude da extensão da lei, bem como para manter os objetivos do presente trabalho, focou-se nos pontos que mais estavam alinhados com as problemáticas já discutidas nos capítulos anteriores.

Na primeira subseção descreve-se um histórico do contexto social e econômico da discussão legislativa da LGPD. Na segunda subseção analisa-se a inegável influência europeia na legislação brasileira, verificando comparativamente os hábitos e os históricos do consumidor europeu *versus* o consumidor brasileiro, tratando-se ainda dos parâmetros para a transferência internacional de dados pessoais. Na terceira subseção verifica-se a problemática do direito à explicação de revisões algorítmicas na legislação, ante a atual disposição da LGPD que não oportuniza a revisão humana de decisões automatizadas. Na quarta seção estudou-se os debates para criação e a atual implementação da Autoridade Nacional de Proteção de Dados, bem como buscou-se verificar a sua futura independência para a proteção do usuário. Por fim, na quinta seção, analisou-se as bases legais instituídas pela Lei Geral, bem como se elas permitem uma desvinculação da utilização do consentimento.

4.1 O Direito e a proteção de dados

A ciência do Direito geralmente está em atraso em relação aos fatos sociais. Para além da questão de regular ou não regular certos aspectos sociais, é claro que o mundo jurídico não alcança a contínua mutação social.

As teorias de Joseph Schumpeter destacam-se ao propor a visão do capitalismo como um sistema dinâmico. Analisando a destruição criativa e a inovação como motor da economia, o autor notabilizou-se pela com-

preensão de uma economia cíclica, que desacelera após um tempo de absorver as inovações (SCHUMPETER, 1997).

De acordo com Norberto Bobbio, a revolução tecnológica no campo das telecomunicações implica em mudanças tais na organização dos indivíduos e nas relações sociais que surgem então situações favoráveis para "o nascimento de novos carecimentos e, portanto, para novas demandas de liberdade e de poderes" (BOBBIO, 2004, p. 53).

Contudo, para evitar a tecnorregulação, ou seja, a dominação do Direito pelas tecnologias e arquiteturas de rede, o Direito deveria regular a tecnologia antes, principalmente por meio de diretrizes éticas. Para alguns, como Edoardo Giannotti, a demora em regular os fatos sociais indica uma necessária inversão dos fatores. "Se o Direito está, efetivamente, colocado na retaguarda dos fatos sociais, é premente a necessidade de uma inversão. A lei não deve apenas proteger a pessoa contra uma realidade que violenta seus valores íntimos" (GIANNOTTI, 1987, p. 17). Para Stefano Rodotà (2008, p. 21), há cada vez mais um aumento da distância entre a velocidade da inovação e o lento planejamento socioinstitucional, gerando obsolescência das soluções jurídicas que se referem a um único dado ou problema.

Muito pretende se falar sobre o impacto de determinadas tecnologias na sociedade. No entanto, consoante explica Pierre Lévy (2010, p. 21), "a metáfora do impacto é inadequada".

A leitura dos fenômenos como impacto pode ser alterada para uma leitura de perspectivas.

Como base da sociedade informacional de Manuel Castells, a internet foi criada nos anos 1960, surgindo, na década seguinte, a preocupação com a manipulação de dados pessoais na Guerra Fria, despontando por isso um ramo legislativo para a proteção da dados. O avanço das telecomunicações e dos computadores, com seu progressivo aumento de armazenamento, proporcionou a verdadeira revolução da tecnologia da informação (CASTELLS, 2008, p. 81).

O direito, portanto, buscando o controle jurídico da revolução informacional, passou à uma onda de leis de proteção de dados, chamadas as leis de primeira geração. Stefano Rodotà (2008, p. 49) assevera que a finalidade das leis dessa geração era responder às preocupações sobre violações da intimidade individual que partiriam dos avanços tecnológicos.

Neste contexto histórico, surgem, segundo Laura Schertel Mendes, a primeira geração de normas de proteção aos dados pessoais: "as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de *Rheinland-Pfalz* (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977)" (MENDES, 2014, p. 30).

O marcante dessas legislações é a indiscutível novidade das tecnologias da informação que surgiram, gerando uma ausência de familiaridade para seu tratamento, bem como a adoção de princípios de proteção amplos e abstratos, focando quase exclusivamente nas atividades de processamento de dados (DONEDA, 2006, p. 208).

Diversos autores defendem, ainda, quatro gerações das normas de proteção dos dados pessoais.[243] A segunda aborda questões sobre o consentimento do cidadão e o exercício de sua liberdade de escolha, em um contexto de Estado Social. A principal diferença em comparação às leis de primeira geração é a melhor compreensão pelos legisladores do fenômeno computacional. Para Danilo Doneda (2006, p. 210), "percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social".

A terceira geração é resultado da proliferação dos bancos de dados interligados, possuindo como marco a decisão do Tribunal Constitucional Alemão (IDEM, p. 210), que declarou inconstitucionalidade em parte da Lei do Censo, surgindo disto alterações na Lei Federal de Proteção de Dados alemã de 1990 e na lei da Noruega, emenda na lei da Áustria de 1986 e previsão constitucional de proteção de dados pessoais na Holanda. Nesta geração alcançou-se o êxtase da própria terminologia do direito à autodeterminação informativa, possibilitando que o indivíduo possuísse um controle mais extensivo sobre suas informações pessoais (BIONI, 2019, p. 116).

Na quarta geração, as normas nacionais sobre proteção de dados são complementadas por normas setoriais suplementares, incluindo-se nela também a Diretiva Europeia sobre proteção de dados de 1995 (95/46/EC), norma precursora do Regulamento Geral sobre Proteção de Dados que entrou em vigor em 2018, mais conhecido como *General Data Protection Regulation* (GDPR). A evolução destes regramentos protetivos tenta evoluir

243 Cf. Mendes (2014, p. 40-44), Doneda (2006, p. 206-213) e Bioni (2019. p. 113-117).

na mesma medida das potências de tratamento de dados dos computadores atuais.

Já existem diversas gerações de leis de dados pessoais na Europa e em alguns países sul-americanos[244] as legislações de dados pessoais já completam duas décadas. Hoje, os principais modelos com maiores diferenças entre si são o norte-americano e o europeu, havendo uma tendência mundial de convergência ao modelo europeu.

Para Danilo Doneda (2006, p. 222-223), mesmo com a diversidade entre os sistemas de *common law* e *civil law*, alguns países adeptos àquele sistema – como Austrália, Nova Zelândia e Canadá – utilizam características mistas na disciplina de proteção de dados pessoais, por vezes aceitando tacitamente a aplicação do direito europeu.

Nos Estados Unidos, por tratar a questão do fornecimento de dados do usuário perante o provedor de forma estritamente contratual, revela-se a posição do país sobre o tratamento de dados pessoais.

O modelo norte-americano "apresenta-se fracionado, com disposições legislativas e jurisprudenciais concorrentes em uma complexa estrutura federativa, o que torna sua leitura em chave sistemática [...] uma tarefa difícil para os próprios juristas norte-americanos" (IDEM, p. 224).

Entre os estados americanos, a Califórnia é um dos com maior nível de proteção à privacidade, já citando este direito no primeiro artigo de sua Constituição. O estado aprovou em 2018 a *California Consumer Privacy Act* (CCPA), com entrada em vigor em 2020, que trata de dados pessoais de consumidores de forma a dar-lhes maior controle sobre suas informações pessoais. A legislação influenciará diversos estados vizinhos, sendo para eles rascunho para futuras leis estaduais de proteção de dados.[245]

Houve a tentativa de passar o que se poderia chamar de lei federal de proteção de dados, o *Do-Not-Track Online Act*, em 2013, requerendo que o FTC regulasse ativamente a coleta e o uso de dados pessoais,

244 Chile e Argentina.

245 STOLTZ, Brenda. A New California Privacy Law Could Affect Every U.S. Business—Will You Be Ready? **Forbes**. 2019. Disponível em: <https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/#79ab352436ac> Acesso em: 6 nov. 2019.

bem como o rastreamento de pessoas na internet. Contudo, a proposta foi arquivada.[246] Em 05 de novembro de 2019, os democratas apresentaram projeto de lei de privacidade *on-line* no Congresso Americano. A Lei da Privacidade *On-line* estabeleceria uma nova agência federal americana, a *Digital Privacy Agency*. Entre os direitos individuais estabelecidos estão o direito de acesso, de correção, de revisão humana de decisões automatizadas e o direito de ser informado.[247] Não se sabe ainda quais as possibilidades de aprovação deste projeto na cultura jurídica estadunidense. Com isso, ainda atual a posição de Stefano Rodotà de que "Vivemos um paradoxo. Importada dos Estados Unidos, a privacidade hoje é mais bem protegida na Europa".[248]

A ânsia brasileira por uma legislação protetiva de dados pessoais já se fazia presente antes mesmo do vigor do GDPR. Inserir-se entre as nações que protegem os dados de seus titulares tornou-se essencial ao jogo político internacional. Para o País se pautar fortemente no regulamento europeu significaria pautar-se em quatro gerações de discussões sobre a proteção de dados pessoais.

A matéria de proteção de dados no Brasil antes da Lei Geral apoiava-se em grande parte em outros ramos do direito como o Código de Defesa do Consumidor, que em seu art. 43 determina: "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". Para Bruno Bioni (2019, p. 128), o Código de Defesa do Consumidor "buscou conferir a autodeterminação informacional, o que perpassa desde regras para garantir a exatidão dos dados até limitações temporais para o seu armazenamento".

246 S. 418 (113th): Do-Not-Track Online Act of 2013. Disponível em: <https://www.govtrack.us/congres s/bills/113/s418> Acesso em: 6 nov. 2019.

247 ESTADOS UNIDOS DA AMÉRICA. Online Privacy Act. 2019. Disponível em: <http://tiny.cc/rvz7fz> Acesso em: 13 nov. 2019.

248 Tradução livre. "*Viviamo un paradosso. Importata dagli Stati Uniti, la privacy è oggi tutelata meglio in Europa*". RODOTÀ, Stefano. Uno statuto giuridico globale della persona elettronica. Discurso proferido na 23ª Conferência Internacional sobre a Privacidade e a Proteção dos Dados Pessoais em Paris. 24 set. 2001. Disponível em: <http://interlex.it/675/rodota5.htm> Acesso em: 11 nov. 2019.

Ainda, a disposição constitucional do art. 5º, LXXII e a Lei n. 9.507/1997, conhecida como Lei do *Habeas Data*, que regulam o direito de acesso a informações, apresentam um dos instrumentos para a proteção de dados pessoais antes da LGPD. Para Danilo Doneda, apesar da possibilidade da utilização do instrumento para proteção, "um sistema de proteção de dados pessoais que tenha como instrumentos principais de atuação o recurso a uma ação judicial [...] não se nos apresenta como um sistema adequado às exigências da matéria" (DONEDA, 2006, p. 337).

A questão também poderia ser abordada pelo Código Civil a partir dos art. 186 "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" e art. 927 "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

A Lei do Cadastro Positivo (Lei n. 12.414/2011) disciplinou de forma setorial a formação de banco de dados relativos a operações financeiras e de adimplemento para fins de concessão de crédito. A peça legislativa trouxe a orientação de que o titular dos dados pessoais deve ter o poder de gerenciá-los e, ainda, que o gestor da base de dados não deve coletar informações excessivas, sensíveis e sem finalidade vinculada (BIONI, 2019, p. 129).

Mais recentemente, em matéria mais aproximada, o Marco Civil da Internet, Lei n. 12.965/2014, regula a tratativa de dados pessoais, como exemplo o art. 3, III que inseriu a proteção de dados pessoais em seus princípios, o art. 7, VII, que informa os direitos dos usuários em não terem seus dados pessoais fornecidos sem consentimento livre ou em possuir informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais. Há ainda referências no art. 11[249] e art. 16.[250]

249 Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...]

250 Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

Contudo, mesmo com uma maior aproximação do Marco Civil, este ainda era consideravelmente limitado por ser aplicável apenas ao ambiente digital. Uma Lei Geral de Proteção de Dados aplica-se em ambiente não somente digital, mas também físico, alcançando em parte o Poder Público e as transferências internacionais.

Assim, uma LGPD brasileira surge não com uma proposta de reestruturação de um sistema já posto, mas sim com a criação de um novo arcabouço jurídico com novos direitos e proteções à estrutura jurídica brasileira. O termo geral não surge como contraposto à uma lei específica, mas sim no sentido de abrangência, regulando todos os setores que porventura se utilizem de dados pessoais.

A discussão de uma Lei Geral de Proteção de Dados Pessoais brasileira se deu por aproximadamente oito anos e pode ser classificada em duas fases.

A fase inicial trata-se de movimentações de órgãos do governo sobre a matéria de proteção de dados pessoais, como o Departamento de Defesa e Proteção do Consumidor – DPDC, publicando o livro intitulado "A proteção de dados pessoais nas relações de consumo: para além da informação creditícia" com a redação de Danilo Doneda em 2010.[251]

Ainda, o Ministério da Justiça cria site destinado a debates de proteção de dados pessoais, apresentando anteprojeto de lei com 48 artigos e incentivando o debate de 30 de novembro de 2010 a 30 de abril de 2011. No total, obteve-se cerca de 2.500 contribuições.[252]

Contudo, a primeira tramitação na Câmara não se deu pelo anteprojeto do Ministério da Justiça, mas sim pelo Projeto de Lei n. 4060/2012, proposto pelo Deputado Milton Monti (PR-SP). O então projeto em nada

I – dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

251 Cf. DEPARTAMENTO DE DEFESA E PROTEÇÃO DO CONSUMIDOR – DPDC. A proteção de dados pessoais nas relações de consumo: para além da informação creditícia. Brasília: SDE/DPDC, 2010. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf> Acesso em: 6 nov. 2019.

252 MINISTÉRIO DA JUSTIÇA. Debate Público Proteção de Dados Pessoais. <http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/> Acesso em: 6 nov. 2019.

assimilava as discussões propostas pelo Ministério da Justiça, possuindo 25 artigos e tratando apenas de direitos do titular e dos requisitos para tratamento de dados pessoais. Entre as justificativas para a tramitação estavam a proteção de direitos individuais, bem como as recentes transformações tecnológicas.

Em 2013 é proposto no Senado Federal o Projeto de Lei n. 330/2013 pelo Senador Antonio Carlos Valadares (PSB/SE) com 19 artigos, focando no direitos dos titulares, tratamento de dados e bancos de dados, citando em sua justificativa o romance 1984 de George Orwell, bem como as denúncias de Edward Snowden.[253]

Em 2014, houve o primeiro grande caso brasileiro de utilização de perfis comportamentais em detrimento do consumidor-usuário, sendo aplicada pelo DPDC multa de R$ 3,5 milhões à TNL PCS S/A (Oi). No caso, foi constatado no processo administrativo que "a parceria da *Oi* com uma empresa britânica *Phorm* consistia no desenvolvimento de *software* que mapeava o trafego de dados do consumidor na internet de modo a compor seu perfil de navegação".[254] Este caso reforçou a necessidade de um caráter punitivista daqueles que atuassem em desobediência às normas de proteção de dados pessoais.

Em 2015, inicia-se a segunda fase, com uma discussão mais técnica e aprofundada, que se manteve até a promulgação da lei em 2018. Ainda em 2015, o Ministério da Justiça disponibiliza o texto do anteprojeto da LGPD com 52 artigos para novo debate público.[255]

Com tramitação lenta até 2015, os esforços estavam centrados na elaboração do Marco Civil da Internet, Lei n. 12.965/2014, que, segundo Bruno Bioni, teve sua tramitação acelerada pelos escândalos de espionagem (BIONI, 2019, p. 131). Segundo o autor:

253 BRASIL. Senado Federal. Projeto de Lei n. 330/2013. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1567533189697&disposition=inline> Acesso em: 1º dez. 2019.

254 MINISTÉRIO da Justiça multa Oi por monitorar navegação de consumidores na internet. Disponível em: <https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet> Acesso em: 6 nov. 2019.

255 MINISTÉRIO DA JUSTIÇA. Proteção de Dados Pessoais. Disponível em: <http://pensando.mj.gov.br/d adospessoais/>. Acesso em: 6 nov. 2019.

> [...] o art. 7º detinha, apenas, cinco incisos, passando a ter, no cenário 'pós-Snowden', oito incisos, sendo que todos eles foram direcionados para a proteção dos dados pessoais. Com o acréscimo de tais dispositivos, houve uma alteração de ordem qualitativa no arranjo normativo do MCI [Marco Civil da Internet], tendo sido o usuário eleito como o grande protagonista para desempenhar a proteção de seus dados pessoais. (IDEM, p. 131)

Também em 2015, o Projeto que tramitava no Senado, n. 330/2013, recebe um substitutivo mais alinhado com o então anteprojeto do Ministério da Justiça.

Fruto das duas consultas públicas, é proposto pelo Poder Executivo o Projeto de Lei n. 5276/2016, com 56 artigos, apresentando esboço mais aproximado ao que se tornaria a LGPD. O Projeto inicial 4060/2012, primeiro projeto apresentado, é consideravelmente diferente do Projeto 5276/2016 do Governo Federal, com grande carga neste da proteção dos consumidores.

Em julho de 2016, os dois projetos de lei que tramitavam de forma concomitante na Câmara foram apensados, sendo criada em outubro do mesmo ano a Comissão Especial para analisar os Projetos de Lei sobre Proteção de Dados Pessoais na Câmara, sob a relatoria do Dep. Orlando Silva (PCdoB/SP), presidência da Deputada Bruna Furlan (PSDB/SP) e vice-presidência pelos deputados André Figueiredo (PDT/CE), Alessandro Molon (Rede/RJ) e Milton Monti (PR/SP). Segundo Bruno Bioni, "essa composição plural com partidos políticos de orientações ideológicas diferentes viria a ser determinante para a aprovação da matéria por unanimidade na Câmara dos Deputados".[256]

Foram realizadas pela comissão especial onze audiências públicas e um seminário internacional, ocorrendo o constante debate de avaliar as diferentes perspectivas da lei e contrapor tanto a visão consumerista como a visão empresarial, movimentando de forma ampla diversos atores sociais.

256 BIONI, Bruno R. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. Jota. 2018. Disponível em: <www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018> Acesso em: 6 nov. 2019.

No ano de 2016, a política brasileira tornou-se especialmente conturbada, tendo em vista o *impeachment* de Dilma Rousseff, ocorrido em 31 de agosto de 2016. As discussões esfriaram, sendo retomadas intensamente em 2018. Além de questões de transferência internacional de dados pessoais trazidas pelo vigor do GDPR, um grande impulsionador da discussão legislativa neste ano foi o desejo brasileiro de tornar-se país-membro da OCDE.

O Brasil apresentou pedido formal de acessão à Organização para a Cooperação e Desenvolvimento Econômico, seguida à execução do programa de trabalho que resultou do Acordo de Cooperação assinado entre o Brasil e a OCDE em 2015.[257] Para tanto, a OCDE desenvolveu análise sobre o Governo Digital brasileiro publicada em 2018, realizando recomendações para atingir um governo digital como estabelecer comunicações "intrafederativas" para expandir de forma consistente o governo digital entre estados e municípios, reforçar as condições para retenção e remuneração de analistas da tecnologia da informação e, entre outras recomendações, disponibilizar múltiplos canais de acesso móvel aos serviços públicos.[258] Em 2019, o Brasil renunciou tratamento especial concedido a países em desenvolvimento pela Organização Mundial do Comércio (OMC), com o objetivo de se tornar parte da OCDE. Até o momento, não houve a aceitação do País como membro.

O ano de 2018 também foi propício para a aprovação da LGPD, ante ao caso de vazamento de dados da *Cambridge Analytica*, havendo, inclusive, requerimento pela Comissão Especial para a análise dos impactos da coleta ilegítima de dados relativa aos projetos que tramitavam na Câmara. Além disso, buscou-se a verificação de como os projetos de lei em análise pela

257 BRASIL. Estratégia Brasileira para a Transformação Digital: E-digital. Brasília: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018. p. 56. Disponível em: <http://www.mctic.gov.br/mctic/export/site s/institucional/estrategiadigital.pdf> Acesso em: 6 nov. 2019.

258 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. Digital Government Review of Brazil. OECD Digital Government Studies, [s.l.]. p.1-146, 28 nov. 2018. OECD. http://dx.doi.org/10.1787/9789264307636-en. Disponível em: <http://www.oecd.org/governance/digital-government-review-of-brazil-9789264307636-en.htm>. Acesso em: 6 nov. 2019.

Comissão poderiam contribuir para evitar e solucionar ações como estas.

Em matéria internacional, em 25 de maio de 2018, o GDPR entrou em vigor. A necessidade de uma legislação de proteção de dados nacional se intensificou ante os obstáculos do Regulamento a transferências internacionais de dados a países que não possuem critérios adequados de proteção.

Em 29 de maio de 2018, a Câmara dos Deputados aprovou por unanimidade a subemenda substitutiva global apresentada pelo deputado Orlando Silva (PCdoB-SP), sendo enviado ao Senado Federal em forma do Projeto de Lei da Câmara n. 53, de 2018, que tramitou em conjunto com o então Projeto de Lei do Senado n. 330 de 2013.

O PLC n. 53/2018 é aprovado em 10 de julho de 2018 e remetido à sanção presidencial, sendo sancionado em 14 de agosto de 2018 com vetos parciais, incluindo nestes o veto à criação da Autoridade Nacional de Proteção de Dados Pessoais, em virtude de que "os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, §1º, II, 'e', cumulado com o artigo 37, XIX da Constituição".[259]

Em 28 de dezembro de 2018, foi publicada a Medida Provisória n. 869/2018, aumentando a *vacatio legis* da LGPD em seis meses, criando a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), entre outras disposições. Também foram alargadas as possibilidades de transferências a entidades privadas de dados pessoais constantes de bases de dados do Poder Público, bem como que a revisão das decisões tomadas unicamente com base em tratamento automatizado de dados pessoais não precisa mais ser feita por pessoa natural. O Projeto de Lei de Conversão n. 7 transformou a medida provisória na Lei n. 13.853/2019.

Percebe-se que a discussão sobre uma normatividade de proteção de dados pessoais se intensificou nos últimos anos mobilizando grandes grupos sociais. Contudo, a discussão permanece após a concretização legal, posto que existem diversas críticas à lei em vigor, como a ausência da especificação de um tratamento diferenciado às microempresas e às empresas de pequeno porte.

259 BRASIL. Presidência da República. Mensagem n. 451, de 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm> Acesso em: 6 nov. 2019.

Pensar em adequação a Lei de Proteção de Dados por essas empresas que lidam com dados em seus recursos humanos ou em uma pequena plataforma de comércio eletrônico, pode evidenciar um distanciamento da legislação da realidade de milhares negócios brasileiros. O tratamento diferenciado das microempresas e empresas de pequeno porte é defendido tanto constitucionalmente quanto pela Lei Complementar n. 123, e é essencial para o desenvolvimento econômico no país.

Comparativamente, o GDPR elencou exceção para pequenas empresas observando quantitativamente o número de empregados, em que, consoante o art. 30, inciso 5, suas obrigações não se aplicam a empresas com menos de 250 funcionários.[260]

Apesar dessas questões, a serem evoluídas com alterações legais ou pela jurisprudência, a importância da LGPD reside no diálogo crescente sobre a matéria, bem como a possibilidade das empresas se adequarem às futuras normas, utilizando-se dessa *vacatio legis* para adequar-se mais ainda ao Código de Defesa do Consumidor e ao Marco Civil da Internet.

Marcos de proteção de dados são normas de natureza exponencial que permitem uma mudança de mentalidade coletiva sobre a importância do tema. A discussão adentrou de forma tão profunda na sociedade que diversos representantes do povo estão propondo projetos de leis municipais e estaduais de proteção de dados pessoais.

Atualmente existem três leis de dados pessoais municipais aprovadas. As dos municípios de Vinhedo (SP) – Lei Complementar 161/2018, João Pessoa (PB) – Lei n. 13.697/2019 e Cariacica (ES) – Lei n. 5.948/2019. Destaque-se que estas leis, em seus artigos iniciais e definidores, são quase cópias da Lei Federal. Ainda estão em discussão leis em dez outros municípios e estados.[261]

Assim, às vésperas da aprovação pelo Congresso Nacional da LGPD,

260 Com a exceção de "que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9º, n. 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10".

261 LEORATTI, Alexandre. Leis de dados pessoais estaduais e municipais: insegurança jurídica à vista? **Jota**. 3 dez. 2018. Disponível em: <https://www.jota.info/especiais/pl-dados-sp-inseguranca-juridica-03122018> Acesso em: 11 nov. 2019.

foi aprovada a PEC 17/2019 para incluir o direito à proteção de dados pessoais no art. 5º da Constituição Federal, estabelecendo-o como direito fundamental. Pretende-se incluir o inciso XII-A "é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais". Como justificativa da proposição cita o GDPR, bem como a constitucionalização desse direito por Portugal, Estônia, Polônia e Chile.[262] Ademais, há a proposição de inclusão do art. 22, inciso XXX, dando competência privativa à União para legislar sobre dados pessoais. A proposição de leis estaduais e municipais que versam sobre o assunto, inclusive replicando a LGPD, provocaria a fragmentação e a pulverização do assunto.

Com isso, percebe-se que a ampla discussão legislativa desenvolveu um documento fruto de amplo debate entre os mais diversos mediadores da sociedade.

4.2 Transferência internacional de dados pessoais e a análise do consumidor europeu *versus* consumidor brasileiro

Transplantes de legislações e doutrinas estrangeiras devem ser vistas com cautela. Consoante a lição de Lena Foljanty (2015, p. 4), a ideia de um transplante remete diretamente a um transplante médico, em que o corpo transplantado pode ou não aceitar o novo órgão. A autora propõe então a utilização do termo tradução cultural para analisar os atores, as suas perspectivas, e o processamento do processo de transferência:

> A metáfora da tradução oferece uma heurística que nos permite fazer perguntas que atualmente não estão no centro da pesquisa relacionada às transferências legais. [...] Ela oferece uma abordagem que nos permite não apenas compreender a complexidade dos processos de transferência, mas também entender como esse processo é moldado pela interação de decisões ativas, pelas mudanças sutis e pela dinâmica interna. Isso nos permite apontar as contradições e falhas ineren-

262 SENADO FEDERAL. Proposta de Emenda à Constituição n. 17 de 2019. 2019. p. 03. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1571776978885&disposition=inline> Acesso em: 11 nov. 2019.

> tes ao processo, bem como examinar seus efeitos na lei e no seu papel na sociedade. No final, todas essas ideias nos permitem verificar como o processo de transferência está expresso na nova lei implementada.[263]

A utilização da metáfora da tradução de um sistema jurídico para o outro, portanto, reflete uma maneira mais acertada de inspirar-se na legislação estrangeira. A doutrina europeia de proteção de dados já foi extensivamente desenvolvida há mais de 30 anos. Por outro lado, a doutrina brasileira engatinha tendo entre as fontes principais doutrinadores e normatividades estrangeiras e uma lei recém-aprovada.

De forma contextual, é importante destacar que o europeu possui inerentemente um maior resguardo ao direito à privacidade. Consoante Marcos Andrey de Sousa,[264] a Europa passou, *há centenas de anos*, a ser palco de inúmeras guerras e conflitos. O cidadão europeu precisava resguardar sua intimidade, sua etnia ou sua religiosidade para garantir a própria sobrevivência. Em pesquisa de 2015, 63% dos cidadãos europeus não confiam em negócios *on-line*, mais da metade não gostam de divulgar dados pessoais em troca de serviços gratuitos e 53% não gostam que empresas *on-line* utilizem os dados pessoais para publicidade direcionada.[265]

Por outro lado, o Brasil possui uma população com hábitos de consumo e de imagem completamente diferentes da população europeia.

---

263 Tradução livre: "*The metaphor of translation offers a heuristic that enables us to pose questions that are currently not at the center of the research concerned with legal transfers.* [...] *It offers an approach enabling us to not only gain an understanding of the complexity of transfer processes, but also for us to grasp how this process is shaped by the interplay of active decisions, subtle shifts, and internal dynamics. It makes it possible for us to point out the contradictions and fault lines inherent to the process as well as to examine their effects on law and on its role in society. In the end, all of these insights enable us to ascertain how the process of transfer is inscribed into the newly implemented law*". (FOLJANTY, 2015 p. 16)

264 As investigações internas e a Proteção de Dados (Lei n. 13.709/18), 05:30 – 06:13 minutos. *In*: IX Congresso Brasileiro de Direito Comercial. São Paulo, 2019. Disponível em: <https://www.congressodireitocomercial.org.br/site/arquivo-de-videos/videos-do-9o-congresso/#video-gallery-b744ef9-22> Acesso em: 12 nov. 19.

265 CABAÑAS, José; CUEVAS, Ángel; CUEVAS, Rubén. Facebook Use of Sensitive Data for Advertising in Europe. Computer Science Cornell University. 2018. Disponível em: <https://arxiv.org/abs/1802.05030> Acesso em: 15 nov. 19.

No País, a autoexposição é cultural, desde os carnavais de rua até a explosão da profissão dos "auto denominados" digitais *influencers*. Não implica nisto um juízo de valor que a cultura brasileira seja inferior, mas *é necessariamente uma diferença cultural que não indica um* mero transplante legal sem uma maior reflexão sobre os hábitos da própria população. Há um marcante componente cultural, na América Latina se introjetam tecnologias de maneira mais acrítica que em outros países. De acordo com Danilo Doneda (2006, p. 28):

> Não é por acaso que a proteção de dados pessoais foi assunto que entrou em pauta primeiramente nos países desenvolvidos: a sensibilidade dos cidadãos para o problema aumenta em proporção aos próprios níveis educacional e financeiro. A comprovar, vide pesquisa conduzida em 1977 ~~na~~ pelo Escritório Nacional de Estatística da Suécia, revelando que a proteção da privacidade era a terceira questão pública mais importante para os suecos (vindo atrás somente do desemprego e da inflação).

O desafio brasileiro será de alcançar a adequação das empresas nacionais que, historicamente, não realizavam medidas de proteção de dados pessoais coletados.

A LGPD é fortemente baseada em fundamentos da regulação europeia. No entanto, a proteção de dados pessoais por meio de legislações e diretrizes de órgãos internacionais é um movimento que se verifica há mais de trinta anos pelo mundo. Assim, a tradução de um sistema que já passou por diversas gerações de análises e de estudos parece mais acertada que tentar uma proposta integralmente diferente e tupiniquim.

Como exemplo, desde 1980, a OCDE possui as diretrizes de proteção de dados chamadas "*Guidelines governing the protection of privacy and transborder flows of personal data*", revisadas em 2013. As diretrizes da OCDE estabeleceram os *Fair Information Practice Principles* (FIPPs)[266], que em grande parte influenciaram as diversas legislações de proteção de dados pelo mundo (BIONI, 2019, p. 121).

266 Nas diretrizes de 2013 os princípios elencados são: *Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle* e *Accountability Principle.*

Inclusive, as diretrizes da OCDE de 1980 influenciaram com muita carga ideológica a Convenção 108 do Conselho da Europa de 1981, a primeira movimentação para harmonizar as legislações europeias sobre o tema (IDEM, p. 122).

Em seguida, em 1995, *é editada a Diretiva Europeia de Proteção de Dados Pessoais (95/46/EC)*. De acordo com Bruno Bioni, a diretiva é fruto direto das diretrizes propostas pela OCDE, adotando os FIPPS como sua espinha dorsal, baseando-se em grande parte na autodeterminação do indivíduo (IDEM, p. 123). Esta Diretiva reflete uma evolução geracional na proteção de dados pessoais, tendo em vista o destaque da participação do indivíduo na proteção dos próprios dados, sendo marco na quarta geração de proteção de dados pessoais (MENDES, 2014, p. 44).

Outro marco da Diretiva Europeia foi a determinação que o tratamento realizado tanto pelo Poder Público, quanto pelo setor privado deveriam estar submetidos ao mesmo regime de proteção. Esta noção foi influenciada pela elaborada doutrina alemã de que os setores públicos e privados deveriam ser regulamentados de forma similar, já que o risco da violação à privacidade existe em ambas as situações. De acordo com Laura Schertel, "a doutrina e a legislação alemãs têm buscado tratar ambos os setores de forma semelhante, sob o fundamento principal de que o direito à autodeterminação informativa do cidadão é único" (IDEM, p. 53).

Em 2012, em virtude do tempo em vigor da Diretiva 95/46, bem como a inerente defasagem legal, a Comissão Europeia realiza a proposição de reforma da diretiva, de forma a fortalecer o direito à privacidade e acelera a economia digital na Europa. *Já em 2014, o Parlamento Europeu demonstrou grande suporte ao regulamento, sendo o RGPD votado em plenário com 621 votos a favor, 10 contra e 22 abstenções.* Dois anos após as normas são aprovadas, em 2016, sendo vinculativa a partir de 25 de maio de 2018.[267] Atualmente, o regulamento europeu busca ser neutro evitando fazer menções a tecnologias específicas, para evitar descompasso no futuro.

267 EUROPEAN DATA PROTECTION SUPERVISOR. The History of the General Data Protection Regulation. 2018. Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> Acesso em: 12 nov. 2019.

De acordo com infográfico da *International Association of Privacy Professionals* – IAPP, após um ano em vigor, os resultados das ações do RGPD resultaram em mais de 56 milhões de euros em multas, mais de 89 mil notificações de vazamento de dados e mais de 144 mil reclamações individuais.[268] Em relatório da Comissão Europeia publicado em julho de 2019, conclui-se que as "empresas estão a desenvolver uma cultura de conformidade, enquanto os cidadãos estão cada vez mais conscientes dos seus direitos".[269]

Contudo, para Winfried Veil o cenário não é exatamente este, já que compara o GDPR ao conto de Hans Christian Andersen "As Roupas Novas do Imperador".[270] O autor aduz que a proteção de dados não passa de um assunto ideológico e que os objetivos do regulamento não são explícitos, sendo quase inconciliáveis.

> Não há uma definição clara do objetivo da proteção de dados. Isso leva a uma grande incerteza jurídica, especialmente na aplicação de obrigações relacionadas a riscos, porque os envolvidos não sabem para qual o 'Schutzgut' protegido (= direito ou interesse) eles devem avaliar os riscos.[271]

---

268 INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. GDPR One Year Anniversary – Infographic. Disponível em: <http://tiny.cc/ae27fz> Acesso em: 12 nov. 2019.

269 VANDYSTADT, Nathalie. Regulamento Geral sobre a Proteção de Dados produz resultados, mas o trabalho deve prosseguir. Comissão Europeia – Imprensa. 2019. Disponível em: <https://ec.europa.eu/commis sion/presscorner/detail/pt/ip194449>. Acesso em: 12 nov. 2019.

270 A história é sobre um imperador que só pensava em vestimentas e na aparência. Dois vigaristas prometeram a ele a mais fina roupa com a qual seria possível distinguir quem não seria adequado a um cargo, já que para os inadequados ela seria invisível. O governante enviou diversas pessoas de confiança para avaliar o trabalho dos supostos tecelões. Contudo, não admitindo elas que não viam nada, mentiram ao imperador sobre a beleza as roupas que supostamente viram. Ao final, o imperador desfila pela cidade nu, até que apenas uma criança aponta que ele não está vestido. (ANDERSEN, 1996)

271 Tradução livre: "*There is no clear definition of the aim of data protection. This leads to great legal uncertainty, especially in the application of risk-related obligations, because those concerned cannot know for which protected "Schutzgut" (= right or interest) they must assess the risks for*". VEIL, Winfried. The GDPR: The Emperor's New Clothes – On the Structural Shortcomings of Both the Old and the New Data Protection Law. *Neue Zeitschrift für Verwaltungsrecht*. Vol. 10, 2018: 686-696. p. 26. Disponível em: <https://ssrn.com/ abstract=3305056> Acesso em: 12 nov. 2019.

O argumento de aumento de custos para as empresas pela adequação à legislação é recorrente. Para Stefano Rodotà, ele não deve prosperar, pois as empresas já suportam outros custos tido como essenciais como segurança dos trabalhadores e a defesa do consumidor. "Não se pode efetivamente estimar que os interesses ligados *à proteção de dados sejam de ordem inferior*" (RODOTÀ, 2008, p. 53).

No mesmo sentido, para Bruno Bioni não se pode apenas olhar para os custos de conformidade, devendo-se focar, em vez, na LGPD como janela de oportunidade, comparando-a ao Código de Defesa do Consumidor:

> A edição de uma lei é apenas o primeiro passo na formação de uma cultura de proteção de dados pessoais no Brasil. Tomando como exemplo a edição do Código de Defesa do Consumidor, nos anos 1990, demorou certo tempo para que o cidadão, os órgãos de fiscalização e os próprios agentes econômicos fizessem a lei pegar. Após quase quatro décadas, é possível dizer que a lei trouxe 'civilidade' ao mercado de consumo, com produtos e serviços mais seguros. As organizações que enxergaram no novo marco regulatório uma oportunidade em agregar valor e reputação aos seus produtos até hoje colhem os frutos de sua estratégia.[272]

A partir do contexto social e histórico europeu, bem como com o aumento da hiperconectividade, há a grande preocupação com a transferência de dados pessoais com países que não necessariamente possuem parâmetros de proteção alinhados com a proteção europeia.

Cumpre ressaltar o que seriam as transferências internacionais. Tudo hoje pode virar transferência internacional pela onipresença da tecnologia. Não é apenas o envio de um material que a caracteriza, mas também o acesso remoto ou qualquer tipo de situação que alguém de fora tem acesso às informações para caracterizar uma transferência internacional, como desde o acesso de uma rede em nuvem para guardar documentos

272 BIONI, Bruno. Inovar pela Lei. **GV-executivo**, v. 18, n. 4, julho-agosto 2019. p. 33. Disponível em: <https://rae.fgv.br/sites/rae.fgv.br/files/gv_0184ce5.pdf> Acesso em: 14 nov. 2019.

até uma curtida no *Facebook*.[273]

As transferências internacionais exigem uma perspectiva global da matéria de dados pessoais, já que sanções podem ser impostas àqueles que, intencionalmente ou não, tratem dados pessoais de cidadãos europeus. Assim, essas transferências são casos de aplicação extraterritorial do regulamento europeu.

Como primeira forma de proteção do compartilhamento internacional de dados pessoais, a Diretiva 95/46/CE utilizou a técnica de proibição de compartilhamento com países terceiros como solução padrão. As exceções caberiam aos países que possuíssem o nível requerido de adequação de legislação. Assim, há uma expansão do escopo da diretiva da União Europeia para todas as empresas estrangeiras processando dados de pessoas residentes na UE.[274] Nesse período inicial da internet, a utilização de transferências internacionais era algo pontual.

---

273 Em julho de 2019, o Tribunal de Justiça Europeu decidiu que os sites que utilizam os botões de *like* do Facebook como *plug-in* devem avisar aos usuários sobre as possíveis coletas de dados. Com um simples *like*, o Facebook transfere dados pessoais automaticamente, algo que pode ser problemático no contexto de transferências internacionais de dados. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Judgment in Case C-40/17 Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. 2019. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf> Acesso em: 12 nov. 2019.

274 Artigo 25: Princípios 1. Os Estados-membros estabelecerão que a transferência para um país terceiro de dados pessoais objecto de tratamento, ou que se destinem a ser objecto de tratamento após a sua transferência, só pode realizar-se se, sob reserva da observância das disposições nacionais adoptadas nos termos das outras disposições da presente directiva, o país terceiro em questão assegurar um nível de protecção adequado. 2. A adequação do nível de protecção oferecido por um país terceiro será apreciada em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados; em especial, serão tidas em consideração a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos projectados, os países de origem e de destino final, as regras de direito, gerais ou sectoriais, em vigor no país terceiro em causa, bem como as regras profissionais e as medidas de segurança que são respeitadas nesse país. [...] 6. A Comissão pode constatar, nos termos do procedimento previsto no n. 2 do artigo 31, que um país terceiro assegura um nível de protecção adequado na acepção do n. 2 do presente artigo em virtude da sua legislação interna ou dos seus compromissos internacionais, subscritos nomeadamente na sequência das negociações referidas no n. 5, com vista à protecção do direito à vida privada e das liberdades e direitos fundamentais das pessoas.

O fato de o conteúdo da Diretiva citar adequação, e não equivalência, significava uma maleabilidade na análise dos países com os quais se poderiam transferir os dados (DONEDA, 2006, p. 28). Assim, os países que receberiam os dados eram aqueles com legislação adequada. Não seria esta legislação uma cópia das normas europeias, mas que na prática a estrutura normativa funcionasse de modo similar, buscando-se evitar, assim, a utilização de paraísos de dados, análogos aos paraísos fiscais, como forma de escape para o tratamento de dados em desconformidade com o regulamento (RODOTÀ, 2008, p. 65).

A dificuldade da implementação dessa barreira, contudo, consistia na relação com os Estados Unidos, um dos principais parceiros comerciais da Europa, que não possuem sistematização na matéria. Desde a promulgação da diretiva, estabeleceram-se grupos de trabalho para adequar a matéria em um patamar comum entre ambas potências, contudo houve parecer negativo sobre a adequação americana em 1999.

Após, para superar a dificuldade em questão, obteve-se um acordo entre as partes chamado de Acordo *Safe Harbour* (Decisão 2000/520) (DONEDA, 2006, p. 318-319). O acordo estabelecia sete princípios básicos para que ocorresse a transferência, sendo eles: a informação do propósito das coletas realizadas; a escolha (*opt-out*) se as informações sobre um indivíduo serão compartilhadas; antes de compartilhar qualquer informação com terceiros, a organização deve seguir os princípios anteriores e assegurar-se que os terceiros também sigam os princípios do *Safe Harbor*; direito de acesso e correção dos dados pessoais; as organizações envolvidas na coleta devem proteger os dados do mau uso, da perda, da alteração e do acesso não autorizado; deve-se atentar ao propósito da coleta de dados realizada; e, por fim, deve ocorrer um *enforcement* dos princípios anteriores e um curso de ação para as organizações que não estão o seguindo.

Este acordo pautou as relações comerciais de ambos os parceiros até 2015, quando o Tribunal de Justiça da União Europeia invalidou o Acordo *Safe Harbour* no chamado o acórdão Schrems[275] tendo em vista, principal-

275 O caso iniciou a partir da demanda de um cidadão austríaco (Schrems) usuário da rede social Facebook, que pediu a proibição da transferência dos seus dados pessoais para aquele país tendo em vista que as práticas estadunidenses não assegurariam proteção suficiente aos seus dados pessoais. TRIBUNAL DE JUSTIÇA DA UNIÃO

mente, os escândalos de espionagem em massa da Agência de Segurança Nacional dos EUA. Em vista disso, as empresas que dependiam do acordo anterior para as operações transatlânticas enfrentaram diversas questões, tendo que se valer de métodos contratuais para alcançar as adequações europeias, dificultando a sua atuação.

De acordo com equipe de pesquisa do Parlamento Europeu, a União Europeia e os Estados Unidos são mercados extremamente interconectados e o cruzamento de dados se verificava em diversos aspectos da vida negocial, envolvendo dados de recursos humanos, transações entre clientes e dados relativos à pesquisa e desenvolvimento.[276] Assim, percebeu-se que entre as duas regiões não era possível que se continuasse sem um acordo de adequação.

Com isso, em 2016 foi negociado um novo acordo bilateral entre as partes, o *Privacy Shield*.[277] O novo acordo levou em conta novas recomendações da União Europeia, o RGPD que estava aprovado e aspectos da decisão do Tribunal de Justiça da União Europeia na decisão que invalidou o *Safe Harbour*.[278] Os princípios anteriormente elencados foram aprimorados, principalmente quanto às situações de *enforcement* dos direitos dos titulares. A *Federal Trade Commission* e as autoridades europeias ficaram com a missão de fiscalizar as transferências realizadas. Assim o acordo atual é um modelo de adesão em que as empresas assim requererem podem se utilizar da estrutura elaborada, sendo responsabilizadas em território americano em caso de descumprimento.

A alteração do *Safe Harbour* para o *Privacy Shield é o início das primeiras* alterações que acompanharam o GDPR. Este, à exemplo da Diretiva ante-

EUROPEIA. Case C-362/14, Maximillian Schrems v Data Protection Commissioner, joined party: Digital Rights Ireland Ltd. 2015. Disponível em: <http://curia.europa.eu/juris/document/documen t.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031> Acesso em: 12 nov. 2019.

276 EUROPEAN PARLIAMENTARY RESEARCH SERVICE. From Safe Harbour to Privacy Shield: Advances and shortcomings of the new EU-US data transfer rules. 2017. p. 11. Disponível em: <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf> Acesso em: 14 nov. 2019.

277 Tradução livre: Escudo da Privacidade.

278 EUROPEAN PARLIAMENTARY RESEARCH SERVICE. Op. cit.. p. 01.

rior, estabeleceu que para que ocorresse a transferência internacional, as disposições do país receptor devem prever um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.[279] Contudo, o nível de proteção parece estar mais rigoroso após o regulamento, eis que o país terceiro deverá ainda ter "nível adequado de proteção essencialmente *equivalente* ao assegurado na União" (grifos nossos).[280]

Além disso, mais uma vez, estará a critério da Comissão Europeia a análise se um país terceiro oferece o nível adequado de segurança jurídica e uniformidade com o direito europeu.[281]

---

279 Considerando (102) O presente regulamento não prejudica os acordos internacionais celebrados entre a União Europeia e países terceiros que regulem a transferência de dados pessoais, incluindo as garantias adequadas em benefício dos titulares dos dados. Os Estados-Membros poderão celebrar acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais, desde que tais acordos não afetem o presente regulamento ou quaisquer outras disposições do direito da União e prevejam um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.

280 Considerando (104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

281 Considerando (103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de

Entre os elementos avaliados pela Comissão, estabelecidos no artigo 45 do Regulamento, estão o primado pelo Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais, a existência de uma legislação de proteção de dados, bem como serão observados os compromissos internacionais assumidos pelo país terceiro. De forma ainda diferenciada, há a previsão de que será levado em conta:

> b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros.

A situação de instalação da autoridade no Brasil, que em um primeiro momento não será independente da Presid*ência da República*, podendo implicar em uma demora no reconhecimento do Brasil como país adequado.

Com isso, denota-se o altíssimo nível de exigências para as transferências internacionais europeias, estabelecendo, ainda, que as avaliações que aprovam um determinado país serão revistas de quatro em quatro anos. Até o momento, foram reconhecidos que possuem proteção adequada apenas os países Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Jap*ão*, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos da América (limitado ao acordo *Privacy Shield*). A adequação da Coréia do Sul está em tramitação. [282]

Caso pretenda-se transferir dados para um país que não seja reconhecidamente adequado, pode-se utilizar de garantias que se traduzem

dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.

282 COMISSÃO EUROPEIA. **Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection.** 2019. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> Acesso em: 14 nov. 2019.

em dois modelos principais, os quais revelam maior utilidade nas transferências internacionais realizadas com regularidade:

> 1. As cláusulas-padrão contratuais (*Standard Contractual Clauses* – SCC), em que o modelo dessas cláusulas é determinado pela Comissão Europeia, assumindo a empresa a total responsabilidade pela proteção destes dados. Apesar do termo cláusula, trata-se de um extenso contrato com inúmeras peculiaridades, mas não há a necessidade de homologação pela Comissão Europeia.[283]
> 2. As normas comparativas globais (*Binding Corporate Rules* – BCR)[284] não se utilizam apenas com o objetivo de transferências internacionais, mas também na transferência entre empresas do mesmo grupo que se situam em diferentes países. Neste documento descrevem-se todas as práticas de proteção de dados utilizadas por uma determinada empresa em âmbito mundial. Essas normas, diferentemente das cláusulas-padrão, devem ser homologadas pela autoridade europeia competente.[285]

Na Lei Geral de Proteção de Dados Pessoais, as transferências internacionais foram estabelecidas no art. 33 e tratadas com o mesmo sistema europeu de adequação. Adicionaram-se aspectos como a possibilidade de transferência quando o controlador oferecer garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na LGPD, quando a transferência for necessária para a proteção

283 COMISSÃO EUROPEIA. **Decisão 2004/915/EC – Standard Contractual Clauses (SCC)**. 2019. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915> Acesso em: 15 nov. 2019.

284 Diferentemente das SCC, as *Binding Corporate Rules* não possuem um modelo a ser seguido. Cada empresa deve formulá-las de acordo com sua política de governança. O *International Association of Privacy Professionals* – IAPP disponibilizam as BCRs aprovadas de algumas empresas globais. INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. **Approved Binding Corporate Rules**. Disponível em: <https://iapp.org/resources/article/approved-binding-corporate-rules/>. Acesso em: 17 nov. 2019.

285 COMISSÃO EUROPEIA. **Binding Corporate Rules (BCR): Corporate rules for data transfers within multinational companies**. 2019. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-prot ection/international-dimension-data-protection/binding-corporate-rules-bcr_en> Acesso em: 15 nov. 2019.

da vida ou da incolumidade física do titular ou de terceiros ou, entre outras situações, quando a autoridade nacional autorizar a transferência.

Também a exemplo do GDPR, o nível do país terceiro será avaliado pela autoridade tendo em consideração as normas gerais e setoriais da legislação em vigor no país de destino; a natureza dos dados; a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na Lei; a adoção de medidas de segurança previstas em regulamento a ser publicado pela ANPD; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais e outras circunstâncias específicas relativas à transferência. Contudo, não há determinação legal de avaliação que no país destino haja uma autoridade eficiente de proteção de dados.

No mesmo padrão europeu, ainda, estabeleceram-se modelos alternativos à adequação, sendo os principais mecanismos de transferência previstos no art. 33 da LGPD: as cláusulas-padrão contratuais; as normas corporativas globais; as cláusulas contratuais específicas para determinada transferência e selos, certificados e códigos de conduta regularmente emitidos.

Com isso, observa-se uma inerente burocratização do trâmite de transferência internacional de dados no Brasil, adotando-se o nível restritivo europeu em um país que não necessariamente possui a mesma cultura de proteção de dados e ainda não possui uma Autoridade Nacional independente.

4.3 Dados pessoais sensíveis e direito à explicação de decisões automatizadas

Como amplamente discutido até o momento, os dados que alimentam as inteligências artificiais são essenciais na moderna lógica de acumulação da informa*ção. Cumpre ressaltar a diferenciação de Danilo Doneda*, para quem informação e dado, apesar de usados de forma sinônima muitas vezes, possuem pesos particulares a serem reconhecidos. Apenas "dado" possui uma conotação mais primitiva e fragmentada, sendo associado à uma pré-informação. Já "informação" alude ao limiar da cognição, em que "a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza" (DONEDA, 2006, p. 152).

A necessidade de uma proteção de dados se dá quando uma informação pode ser vinculada à uma pessoa, consequentemente revelando algum aspecto objetivo desta (IDEM, p. 153). Assim, a definição de dados pessoais na lei brasileira, consoante disposto em seu art. 5º, é "informação relacionada a pessoa natural identificada ou identificável". Esta definição se mostra consideravelmente reduzida quando contraposta com a definição de dados pessoais do RGPD:

> "Dados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Assim, dados pessoais seriam dados de localização, dados financeiros, hábitos de consumo, características físicas etc. Percebe-se que no Brasil optou-se por uma definição mais sintética de dados pessoais, para criar um subgrupo desses dados: os dados pessoais sensíveis.

Dados pessoais sensíveis sequer são citados pelo RGPD pois já estão incluídos na própria definição de dados pessoais.

Danilo Doneda, autor que possuiu grande influência na redação da Lei Geral, principalmente no anteprojeto apresentado pelo Ministério da Justiça, já esclarecia em seu livro que a categoria de dados sensíveis foi criada pela prática do direito da informação. Estes dados seriam as informações conhecidas e processadas que se prestariam a ser utilizadas como um potencial discriminatório. O autor afirma que estes dados são frutos de uma observação pragmática da diferença do tratamento destes em relação aos demais, contendo um "elevado potencial lesivo aos seus titulares, em uma determinada configuração social" (DONEDA, 2006, p. 161).

Dado pessoal sensível na LGPD é:

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de

> caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Ainda há incerteza se o rol acima seria taxativo ou exemplificativo. O reconhecimento sobre um ou outro irá depender do funcionamento da Autoridade Nacional, contudo, por não haver indicativos na própria lei, a tendência enquanto isto é do reconhecimento como rol taxativo.

Para Bruno Bioni, os vocábulos utilizados pela LGPD definem dado pessoal a partir de uma visão expansionista, que alargam a qualificação do dado como pessoal. Uma visão reducionista se utilizaria apenas das fórmulas: pessoa identificada, específica ou determinada com vínculos imediato, direto, preciso ou exato. Contudo, utilizou-se na legislação os termos "identificável" para alcançar uma maior gama de titulares, bem como "pessoa indeterminada, com vínculo mediato, indireto, impreciso ou inexato (BIONI, 2019, p. 68).

Existe, ainda, a possibilidade que um dado se refira a uma pessoa indeterminada. Estes seriam os dados anônimos. Geralmente para um dado se tornar anônimo é feito um tratamento a partir de dados pessoais, realizando-se uma "anonimização"[286], em que são retirados os vínculos capazes de identificar uma pessoa natural.

Para a LGPD, dado anônimo é "relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;"[287] e a anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;".[288]

Em regra, consoante o art. 12[289] da Lei Geral, os dados anônimos não

286 Danilo Doneda (2006, p. 157) utiliza-se do termo "anonimação".

287 Art. 5º, III, Lei Geral de Proteção de Dados Pessoais.

288 Art. 5º, XI, Lei Geral de Proteção de Dados Pessoais.

289 Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

serão considerados dados pessoais. Contudo, reconhece a legislação a possibilidade da reversão da anonimização, sendo, nestes casos, os dados protegidos. Também no RGPD os princípios de proteção de dados não se aplicarão às informações anônimas.[290]

Um dado pseudoanonimizado pode ser classificado como dado pessoal, pois em sua definição: "a pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro".[291]

Com isso, a única semelhança entre dado anonimizado e pseudoanonimizado é o sufixo, pois neste o controlador pode refazer a cadeia de dados e reconfigurar os códigos em informação identificadora. Como exemplo gráfico da identificação de dados pessoais sensíveis, dados pessoais e dados anonimizados está a figura abaixo:

290 Considerando (26) [...] Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

291 Art. 13, § 4º, Lei Geral de Proteção de Dados Pessoais.

FIGURA 13 – DADO ANONIMIZADO, DADO PESSOAL E DADO PESSOAL SENSÍVEL

Fonte: INSTITUTO DE TECNOLOGIA E SOCIEDADE. Lei Geral de Proteção de Dados Pessoais (LGPD) e Setor Público: Um guia da Lei 13.709/2018, voltado para os órgãos e entidades públicas. Rio de Janeiro: ITS, 2019, p. 13. Disponível em: <http://tiny.cc/uaqugz> Acesso em: 25 nov. 2019

A reversão de dados anonimizados é uma realidade em muitos casos. Assim, a garantia com eficiência do anonimato das pessoas não passa de um mito (BIONI, 2019, p. 73). Em pesquisa de Yves-Alexandre de Montjoye *et al.*, a partir da análise de movimentações financeiras do cartão de crédito de indivíduos, verificaram a "reidentificabilidade" de um dado anônimo. Partindo da ideia de que em alguns países como os Estados Unidos[292] as movimentações financeiras são os dados pessoais mais sensíveis mundialmente,[293] os autores analisaram as transações de 1,1 milhões de usuários em dez mil lojas em um país da OCDE.

Como exemplo, partindo de uma base de dados anonimizadas, conseguiam identificar um indivíduo que foi a uma padaria no dia 01 do mês e a um restaurante no dia 02 do mês, pois os locais e os valores das transações tornavam os dados altamente reidentificáveis. A pesquisa mostrou

292 Tendo em vista o grau de consumo dos cidadãos e a alta incidência de pagamento por meio de cartão de crédito.

293 MONTJOYE, Y.-a. de et al. Unique in the shopping mall: On the reidentifiability of credit card metadata. **Science**, [s.l.], v. 347, n. 6221. p.536-539, 29 jan. 2015. American Association for the Advancement of Science (AAAS). p. 537. Disponível em: <https://science.sciencemag.org/content/347/6221/536/tab-pdf>. Acesso em: 15 nov. 2019.

ainda que mulheres são 1.214 vezes mais fáceis de serem identificadas que homens e pessoas com maiores rendas são 1.746 vezes mais identificáveis que pessoas de baixa renda.[294]

Com isso, percebe-se que o dado anônimo, pela sua alta insegurança na proteção do titular dos dados, deveria ser reconhecido como dado pessoal e protegido de acordo. Para Bruno Bioni, a dicotomia entre dados pessoais e dados anônimos só possuiria coerência se a legislação tivesse adotado o conceito reducionista de dados pessoais, o que não foi o caso, já que se criou o subgrupo de dados pessoais sensíveis. De acordo com o autor, "leis que adotam o conceito expansionista de dados pessoais e, ao mesmo tempo, estabelecem uma dicotomia deste com dados anônimos correriam o risco de ser tautológicas" (BIONI, 2019, p. 75).

A LGPD utiliza-se do critério da razoabilidade para analisar um risco aceitável-tolerável (IDEM, p. 76) da reversibilidade dos dados anônimos, consoante art. 12, § 1º:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

Com isso, a legislação busca extinguir essa dicotomia a partir do fator da razoabilidade, impedindo uma redundância normativa, já que dados anônimos sem o critério da razoabilidade em sua reversão seriam considerados dados pessoais (IDEM, p. 77).

O Superior Tribunal de Justiça já reconheceu no RESP n. 1.419.697/RS a possibilidade de utilização de dados pessoais consumidor em análise de risco de crédito, culminando na Súmula 550:

294 Idem, p. 538.

> A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.[295]

Contudo, antes o Tribunal já havia estabelecido limites a essa análise, em julgamento de recursos repetitivos à sensibilidade de avaliações de risco de crédito, em que deverão ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor para a tutela da privacidade, bem como a máxima transparência nas relações comerciais.[296] Na mesma decisão analisou-se o direito à explicação do consumidor, em que "devem ser a ele fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas".[297] As informações sensíveis também foram protegidas da forma que não deverão ser analisadas, na análise de crédito, as informações "relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, **ou excessivas**, como as referentes a gostos pessoais, clube de futebol de que é torcedor etc.[298] [grifos do autor]

Todas essas informações agrupadas podem se tornar um perfil comportamental, consoante exaustivamente delineado na subseção 3.2 do presente trabalho. Este perfil será tanto mais complexo quanto maior o número de informações nele abrangidas. Nisto, releva-se a necessidade de o perfil ser reconhecido como dado pessoal, eis seu caráter potencialmente identificativo do titular, como é o caso da técnica de *fingerprinting*.

Os perfis comportamentais são abrangidos na LGPD como uma extensão da classificação de dados pessoais, desde que seja referente à

295 BRASIL. Superior Tribunal de Justiça. Súmula 550. Brasília/DF, 14 de outubro de 2015. **Diário Oficial**. Brasília, 19 out. 2015. Disponível em: <https://scon.stj.jus.br/SCON/sumanot/toc.jsp?livre=(sumul a%20adj1%20%20550).sub.>. Acesso em: 18 nov. 2019.

296 Idem. Superior Tribunal de Justiça. Recurso Especial n. 1.419.697. Relator: PAULO DE TARSO SANSEVERINO. Brasília/DF, 12 de novembro de 2014. **Diário Oficial**. Brasília, 17 nov. 2014. p. 37. Disponível em: <http://tiny.cc/kvhdgz>. Acesso em: 16 nov. 2019.

297 Idem, ibidem. p. 37.

298 Idem, ibidem. p. 36.

uma determinada pessoa natural e identificada.[299] Contudo, restaram de fora os perfis comportamentais de pessoas potencialmente identificáveis em que basta, por exemplo, o cruzamento de uma base de dados com outra para a sua identificação.

A adoção de um aspecto reducionista neste ponto da legislação pode fragilizar de sobremaneira a proteção dos direitos do titular de dados pessoais. A utilização massiva de perfis comportamentais para os mais diversos propósitos, desde publicidade comportamental até análise de crédito, revela que estes mereciam uma maior proteção legal, com o reconhecimento de serem dados pessoais da pessoa identificada ou identificável.

No RGPD o tratamento se deu de forma mais cuidadosa, optando-se pela criação de uma definição de perfil comportamental, em que seria:

> [...] qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

Esta definição de perfil não abrange um aspecto reducionista, eis que não vincula a proteção apenas às pessoas identificadas. Os perfis comportamentais são amplamente citados no RGPD, diferentemente da lei nacional, que apenas os menciona em dois momentos.

No RGPD, por exemplo, o responsável pelo tratamento de dados pessoais deve fornecer ao titular informações sobre a existência de decisões automatizadas a seu respeito, estando esse direito destacado ainda no artigo sobre direito de acesso do titular dos dados.[300] Ainda no regu-

299 Art. 12. [...] § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

300 Art. 13, 2, f: A existência de decisões automatizadas, incluindo a definição de perfis, referida no art. 22, nos 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

lamento, é estabelecido direito de oposição do titular dos dados ao tratamento de seus dados, incluída neste direito também a noção de perfil comportamental.[301] É interessante ressaltar que o titular não será obrigado a ficar sujeito a nenhuma decisão tomada com base no tratamento automatizado que produza efeitos na sua esfera jurídica.[302]

A segunda menção ao perfil comportamental na LGPD é no tocante ao art. 20, que desde a sua promulgação, já foi alterado por duas vezes.

A redação inicial do art. 20 era:

> O titular dos dados tem direito a solicitar revisão, **por pessoa natural**, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (grifos nossos)

A inclusão da revisão por pessoa natural coaduna-se com o estado da arte da inteligência artificial, em que as máquinas ainda não são capazes de ter a cognição humana suficiente para reconhecer excessos ou injustiças. Como o caso citado na subseção 3.2.1 em que a idosa era continua-

---

A redação se repete no art. 14., 2, g e art. 15, 1, h.

301 Art. 21. **Direito de oposição** 1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no art.6º, n. 1, alínea e) ou f), ou no art.6º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta. [...]

302 Art. 22. **Decisões individuais automatizadas, incluindo definição de perfis**
1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. [...]

mente negada em asilos comunitários por supostamente possuir registros de prisão, outros casos relativos aos mais diversos aspectos da vida social podem surgir das decisões automatizadas sem revisão por pessoa natural.

A primeira alteração do art. 20 se deu com a Medida Provisória n. 869/2018 que retirou a expressão "por pessoa natural", indicando apenas que o titular poderia solicitar revisão. No Projeto de Lei de Conversão n. 7/2019, que posteriormente tornou-se a Lei n. 13.853/2019 que alterou a LGPD, a redação do caput sem o termo pessoa natural foi mantida, permanecendo o §3º: "A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados".

Contudo, o parágrafo acima foi vetado pelo Presidente da República sob o argumento:

> A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.[303]

A observação apenas dos efeitos econômicos não plausíveis da revisão por pessoa natural, quando sequer há espaço na legislação para as microempresas e as empresas de pequeno porte, releva a desconsideração pelos efeitos mais amplos que a mera revisão automatizada pode acarretar. Infelizmente, em 2 de outubro de 2019, a votação do Congresso

303 BRASIL. Presidência da República. **Mensagem n. 288/2019**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm>. Acesso em: 17 nov. 2019.

Nacional dos vetos presidenciais manteve o veto para afastar a obrigatoriedade de revisão humana sobre decisões tomadas unicamente com base em tratamento automatizado de dados.

Para a derrubada do veto era necessária apenas a maioria simples dos votos tanto na Câmara dos Deputados quanto no Senado Federal. Aquela aprovou a derrubada, mas no Senado Federal, com 15 senadores favoráveis ao veto presidencial, este se manteve por 1 voto.[304]

Vale ressaltar que, no *Online Privacy Act*, projeto americano de proteção de dados pessoais, a proposta inclui entre os direitos dos titulares o direito à revisão humana de decisões automatizadas.[305]

Assim, o atual veto à revisão por pessoa natural de decisões automatizadas revela inerente descompasso com a proteção de dados pessoais pretendida. O direito do titular de requerer revisão, sem maiores explicações sobre como esta é realizada, torna o direito inócuo, eis que por muitas vezes as decisões tomadas por inteligência artificial *são ininteligíveis.* Por vezes, a análise a partir do *big data* se forma a partir de um volume tão expressivo de dados que se torna impossível explicar a razão de uma determinada decisão automatizada.

Disto se destaca a importância do direito à explicação nas decisões automatizadas. Para Renato Leite Monteiro (2018, n. 39. p. 1-17), o qual deriva do princípio da transparência, consoante estabelecido na própria LGPD no art. 5º, VI: "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

Contudo, o princípio da transparência e, consequentemente, o direito à explicação, restam cada vez mais seriamente prejudicados pelas formas que o *machine learning* é programado. A tentativa de criar máquinas cada vez mais adaptáveis e com respostas similares às respostas huma-

304 BRASIL. Congresso Nacional. Veto n. 24/2019 – Votação do dispositivo 24.19.001 – § 3º do art. 20 da Lei n. 13.709, de 14 de agosto de 2018, com a redação dada pelo art. 2º do projeto. Disponível em: <https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445/1>. Acesso em: 17 nov. 2019.

305 ESTADOS UNIDOS DA AMÉRICA. **Online Privacy Act**. 2019. Disponível em: <http://tiny.cc/rvz7fz> Acesso em: 13 nov. 2019.

nas encerra-lhe um comportamento menos previsível. Assim, elas desenvolvem suas próprias lógicas internas, de forma menos controlada pelos agentes humanos (MAGRANI, 2019, v. 8, n. 3, p. 5).

Apesar do atual estado da arte da tecnologia ainda não ser capaz de tomar decisões autônomas, aduz Eduardo Magrani que cada vez mais será possível criar máquinas que decidam de forma mais autônoma, levantando questões sobre a responsabilidade por seus atos (IDEM, p. 5).

A utilização dos algoritmos está cada vez mais opaca, no sentido de que os humanos não conseguem prevê-los, explicá-los ou entender seus funcionamentos, seus preconceitos e seus problemas. De acordo com Danilo Doneda e Virgílio Almeida (2016, v. 20, n. 4, p. 60-63), existem razões técnicas e não-técnicas pela ocorrência da opacidade dos algoritmos. Entre as não-técnicas estão:

> Algumas delas [razões não-técnicas] possuem fundamento em questões de concorrência. Ter um algoritmo aberto pode colocar uma empresa em desvantagem em relação a seus concorrentes. Outras são baseados em propriedade intelectual: em alguns países, a lei protege o segredo comercial ou a propriedade intelectual de uma empresa. Outro motivo para não expor determinados algoritmos é a possibilidade de que algumas pessoas – depois de conhecerem suas características – possam 'melhorar' o algoritmo.[306]

Assim, diante destas questões de inacessibilidade algorítmica, os autores propõem uma "governança algorítmica". Essa governança focaria em *accountability*, na transparência e nas garantias técnicas. As ferramentas dessa governança devem variar de acordo com a situação, mas algumas, por exemplo, focam nos dados que alimentam os algoritmos, não nestes em si (IDEM, p. 61).

306 Tradução livre: "*Some of them are based on issues over competition. Having an open algorithm could put a company at a disadvantage regarding its competitors. Others are based on intellectual property: in some countries, the law protects a company's commercial secret or intellectual property. Another reason for not opening certain algorithms is the possibility that some people – once they're aware of their characteristics – could be able to better 'game' the algorithm*". (DONEDA; ALMEIDA, 2016, v. 20, n. 4, p. 61)

No mesmo sentido de "governança algorítmica", a autoridade do Reino Unido, *Information Commissioner's Office* (ico.), publicou trabalho sobre *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. De acordo com a autoridade, diversas técnicas devem ser utilizadas para evitar uma constante opacidade algorítmica. Entre elas seria a de auditor algoritmos para identificar os fatores que influenciam suas decisões; criar visualizações interativas aos usuários para ajudá-los a entender certas recomendações automatizadas; comitês de ética também podem ser utilizados para moldar e melhorar a transparência no desenvolvimento de algoritmos de *machine learning* e buscar combinar aspectos técnicos e organizacionais para obter a transparência algorítmica.[307]

Em abril de 2019, um grupo independente de peritos de alto nível sobre a inteligência artificial foi reunido pela Comissão Europeia para criar as Orientações Éticas para uma "IA de Confiança". De acordo com o grupo, para promover uma "inteligência artificial de confiança", esta deve ser cercada de três componentes: deve ser legal, de forma a cumprir as legislações e regulamentos aplicáveis; deve ser ética, com observância de princípios e valores éticos; e deve ser sólida, tanto do ponto de vista técnico quanto do ponto de vista social.[308]

Para além dessas propostas, Sandra Wachter e Brent Mittelstadt pretendem proporcionar uma maior elucidação desses modelos, sem propriamente desvendá-los, criando o direito a inferências razoáveis. Aduzem os autores que a transparência e a explicação de uma decisão só podem ser realizadas após ela já ter sido tomada. Com isso, as explicações do modelo, em si, não garantem que uma decisão algorítmica é justa (WACHTER; MITTELSTADT, 2019, n. 2, p. 12).

Os autores criticam que a atual regulamentação da União Europeia não considera a amplitude de riscos na análise de dados com o *big data*

307 REINO UNIDO. Information Commissioner's Office. **Big Data, Artificial Intelligence, Machine Learning and Data Protection**. 2017. p. 86. Disponível em: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf> Acesso em: 18 nov. 2019.

308 UNIÃO EUROPEIA. Comissão Europeia. **Orientações Éticas para uma IA de Confiança**. 2019. p. 02. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai> Acesso em: 18 nov. 2019.

analytics, com isto, tal direito busca uma solução das métricas confusas de dados pessoais, de dados pessoais sensíveis e de dados anonimizados (IDEM, p. 88).

Com isso, o direito a inferências razoáveis protegeria os cidadãos das inferências do *big data analytics* que : "(1) estão previstas ou demonstradas à causar danos à reputação ou à invadir a privacidade de alguém, e (2) têm baixa verificabilidade no sentido de serem preditivas ou baseadas em opiniões enquanto estiverem sendo usadas para obter decisões importantes".[309]

A possibilidade de prejuízo aos cidadãos que são submetidos à uma decisão algorítmica opaca é inerente quando esta é utilizada, principalmente quando ainda resta dificuldade em obter dos dados as explicações das tomadas de decisões. Além da possibilidade de algoritmos com vieses discriminatórios, há a problemática quando a obtenção de dados na internet se dá, na maioria das vezes, à revelia do usuário.

Muitas vezes, o cidadão apenas se vê com a necessidade de um direito à explicação quando é implicado negativamente em análises de crédito. Por esta razões, a maioria das decisões em tribunais superiores dizem respeito a ações que surgiram em face de uma discriminação monetária. As outras formas de discriminação, que podem passar despercebidas pelo indivíduo, são essencialmente danosas se analisadas do ponto de vista social. Assim, a defesa de uma cultura de proteção de dados engloba também o direito à explicação.

O direito à explicação com base em decisões algorítmicas pode ser inferido do princípio da transparência elencado na LGPD, de forma a criar uma razoabilidade na interpretação de como a revisão das decisões automatizadas deveria se dar. A grande proteção de dados pessoais pretendida pela legislação pode restar ineficaz se não observados os algoritmos que permeiam a vida social.

309 Tradução livre: *"(1) are predicted or shown to cause reputational damage or invade one's privacy, and (2) have low verifiability in the sense of being predictive or opinion-based while being used to make important decisions*". (WACHTER; MITTELSTADT, 2019, n. 2, p. 90).

4.4 A Autoridade Nacional de Proteção de Dados e a sua independência para a proteção dos direitos do usuário

A Lei Geral de Proteção de Dados Pessoais, por ser amplamente inspirada na evolução da doutrina europeia, insiste em uma autorregulação e na aplicação de práticas de *compliance.*

Para além da evolução doutrinária da proteção de dados pessoais, é preciso destacar que nos moldes sociais atuais a tecnologia é também vetor de regulação. Esta, conforme o caso, pode mitigar ou neutralizar a regulação jurídica e decisões judiciais.

Como explicado no subitem anterior, a dinâmica da inteligência artificial por vezes não é passível de compreensão e explicação. Além disso, a dinâmica de comunicações criptografadas, por vezes, não pode ser desvendada facilmente, tanto por questões da política de privacidade dos usuários de determinada rede quanto por barreiras na própria tecnologia. Como exemplo, estão as frequentes decisões de retirada do aplicativo *WhatsApp* do ar no Brasil.[310]

A tecnologia, em seu estado da arte, pode ser uma barreira quase intransponível à regulação jurídica, já que a escolha desta não é necessariamente neutra e pode ser criada para prejudicar direitos dos titulares sob um pretexto de sua inteligibilidade.

Neste contexto social e tecnológico, uma autoridade de proteção de dados pessoais é medida essencial para que a proteção deste ramo do direito seja resguardada de forma administrativa. Um órgão isento e independente garante aos titulares dos dados pessoais a efetiva proteção de

310 Ocorreram, até o momento, quatro bloqueios do aplicativo de mensagens do grupo do Facebook. O primeiro, de fevereiro de 2015, não foi cumprido antes da liminar ser revogada; o segundo, em dezembro de 2015, ocorreu em um processo criminal que corria em segredo de justiça e o aplicativo ficou fora do ar por 14 horas; a terceira vez, em maio de 2016, também por um processo criminal, ficando o aplicativo fora do ar por 24 horas e a quarta vez, em julho de 2016, em outro processo criminal, com a ordem do aplicativo interceptar mensagens de crimes na região. WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. **Portal G1**. São Paulo, jul. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html>. Acesso em: 24 nov. 2019.

seus direitos, que são, entre outros, os incisos do art. 18 da LGPD:

> I – confirmação da existência de tratamento;
> II – acesso aos dados;
> III – correção de dados incompletos, inexatos ou desatualizados;
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V – 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;
> VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX – revogação do consentimento

Assim, uma autoridade de proteção de dados é essencial para que a lei seja interpretada de forma sistemática e unitária, já que hoje desde a coleta ao descarte há o tratamento de dados pessoais.

A criação de uma autoridade se deu de forma complexa no Brasil. No primeiro projeto apresentado, Projeto de Lei n. 4060/2012, a única menção a qualquer autoridade se dava em seu art. 24,[311] que informava que os direitos previstos na lei não excluíam outros de outras leis ou regulamentos de outras autoridades. Já no Projeto de Lei n. 5276/2016, citava-se a necessidade de um órgão competente, bem como a criação de um Conselho Nacional de Proteção de Dados Pessoais.

A partir da evolução da discussão legislativa, bem como da análise dos

311 Art. 24. Os direitos e obrigações previstos nesta lei não excluem outros, decorrentes de tratados ou convenções internacionais de que o Brasil seja ou venha a ser signatário, da legislação interna ordinária, bem como de regulamentos expedidos pelas autoridades administrativas competentes.

parâmetros europeus para transferência internacional de dados pessoais, denotou-se que seria necessária uma "Autoridade de Proteção" forte e independente. Com isso, a LGPD foi aprovada pelo Congresso Nacional contendo em seus artigos 55 a 57 as disposições da Autoridade Nacional de Proteção de Dados (ANPD). A legislação, contudo, não foi aprovada sem vetos.

Entre os vetos presidenciais, o mais sensível se deu em relação à Autoridade Nacional de Dados Pessoais, em que houve a completa fragilização do sistema sancionatório da Lei, deixando a legislação sem efetividade prática, já que a lei precisaria ser largamente regulamentada pela autoridade para possuir uma aplicabilidade razoável. Na comparação de Rafael Zanatta em entrevista: "É como se a vigilância sanitária não pudesse fechar um restaurante com coliformes fecais na cozinha".[312] As razões do veto foram vício de iniciativa, já que o Poder Legislativo propôs a criação de despesa ao Poder Executivo, em que a autoridade permaneceria vinculada.

Quatro meses após os vetos, a ANPD finalmente foi criada por meio da Medida Provisória n. 869/2018, convertida na Lei n. 13.853/2019 que altera a LGPD. O conselho diretor, órgão máximo de direção, será composto de cinco diretores, incluído o diretor-presidente. Foi criado ainda o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade composto de 23 representantes. Suas prerrogativas, entre outras, são as de sugerir ações a serem realizadas pela Autoridade, elaborar relatórios e estudos sobre privacidade e proteção de dados, propor diretrizes e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade. Foram indicados até o momento, na vaga da Câmara dos Deputados, a indicação de Danilo Doneda e Fernando Santiago nas posições de representante titular e suplente.[313]

Assim, a Autoridade foi criada sem aumento de despesa, órgão da administração pública federal e integrante da Presidência da República. Sua natureza jurídica é transitória e, consoante o §1º do art. 55-A, "poderá

312 PAYÃO, Felipe. Michel Temer, finalmente, cria Autoridade de Proteção de Dados. **Tecmundo**. São Paulo, dez. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/137510-michel-temer-cria-autoridade-protecao-dados-brasileiros.htm>. Acesso em: 24 nov. 2019.

313 BRASIL. Câmara dos Deputados. Ato da Presidência de 15/10/2019. **Diário Oficial da Câmara dos Deputados**. Disponível em: <http://tiny.cc/xqhsgz> Acesso em: 24 nov. 2019.

ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República".

Entre críticas, sugere-se que a ANPD deveria ser vinculada ao Ministério de Justiça, e não à Presidência da República, eis que se pretende que a sua atuação seja nos mesmos moldes técnicos do Conselho Administrativo da Defesa Econômica (CADE).

A necessidade de independência da autoridade reflete sua própria razão de ser e, consoante Danilo Doneda, é realizada:

> por meio de mecanismos que afastem o máximo possível a sua atuação da influência dos poderes estatais constituídos. [...] Outro mecanismo para operar sua independência é a ausência de ingerência governamental sobre seus atos, que se pode obter situando tais órgãos fora de uma posição hierárquica em relação ao governo. (DONEDA, 2006, p. 393)

Uma situação crítica à independência da Autoridade Nacional de Dados Pessoais se dá pela sua demasiada proximidade ao Poder Executivo. O interesse estatal nos dados dos seus cidadãos tanto para fins de políticas públicas, mas também com outros fins de vigilância e de fiscalização, foi a base do desenvolvimento da doutrina de proteção de dados, a exemplo da decisão alemã contra um censo invasivo, criando o direito à autodeterminação informativa.

Apesar da LGPD, em seu art. 4º, III, expressamente limitar o alcance da lei e não tratar de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ainda existem diversas formas de utilização e tratamento de dados em âmbito estatal que podem se pautar pela legislação.

O papel da autoridade no tratamento de dados pelo Poder Público se revela diversas disposições da Lei Geral, destacando-se o art. 32 em que estabelece que a Autoridade Nacional poderá solicitar às entidades do Poder Público informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado, bem como no art. 29 que indica que "A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados

pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público".

Contudo, em descompasso com a discussão de proteção de dados no Brasil, o Decreto n. 10.046/2019 foi publicado e já está vigente, dispondo sobre a governança no compartilhamento de dados no âmbito da administração pública federal e instituindo o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Neste decreto, os direitos dos titulares são mencionados como meros limites, sem uma real legitimidade a esse sistema de tratamento.[314] O decreto aparenta ainda estar em descompasso com a LGPD pelo seu art. 26: "O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei".

Ademais, o mais problemático deste decreto é a criação de uma base integradora, que na definição é uma base de dados que integra os atributos biográficos ou biométricos das bases temáticas.[315] Ainda, os dados biométricos comportamentais são citados pela primeira vez em uma legislação brasileira, chegando-se à definição destes como: "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;" [316]

A criação de uma base única do cidadão vai de encontro aos princípios elencados na disciplina de proteção de dados pessoais brasileira e amplamente debatido pela sociedade nos últimos oito anos. Enquanto a

314 Danilo Doneda em entrevista à Cristina De Luca. DE LUCA, Cristina. Decreto de Bolsonaro aproxima uso de nossos dados a países como China. Blog Porta 23. **Uol**. Rio de janeiro, outubro de 2019. Disponível em: <https://porta23.blogosfera.uol.com.br/2019/10/13/governo-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles> Acesso em: 24 nov. 2019.

315 Bases temáticas, na definição do art. 2º, VII: "base temática – base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora;"

316 Art. 2º, II.

LGPD elenca hipóteses restritas de tratamento de dados e, consequentemente, a minimização dos dados, o decreto busca a maximização da coleta de dados, inobservados os princípios da finalidade[317] e da necessidade. No mesmo mês em que foi emitido, há movimentações na Câmara dos Deputados para sustar efeitos do decreto presidencial.[318]

O tratamento de dados pessoais está na essência dos estados modernos, contudo isto deve ser realizado de forma cautelosa e amplamente estudada, propiciando, principalmente, o desenvolvimento da segurança da informação.

Destaque-se que os dados de 70 milhões de brasileiros foram vazados, em outubro de 2019, pelo Detran (RN), em que foi possível acessar as bases de dados de todos os Detrans do país. Diversos dados sensíveis como endereço residencial, telefone, dados da CNH – como categoria, validade, emissão, restrição, registro.[319]

Vale destacar, ainda, que entre os maiores vazamentos de uma base de dados estatal está o da base do governo indiano, *Aadhaar,* que continha tanto informações demográficas como informações biométricas. As informações básicas eram disponibilizadas a quem pagasse o valor de $8,00 (oito dólares). O próprio cartão de identificação poderia ser disponibilizado para impressão mediante o pagamento de $5,00 (cinco dólares).[320] A fragilidade da junção de uma base de dados única dos cidadãos, portan-

317 O princípio da finalidade abrange situações em que o agente de tratamento deve ter uma finalidade específica para a coleta e tratamento de dados, não podendo esta finalidade ser genérica ou utilizados os dados para finalidade distinta.

318 SOPRANA, Paula. Deputados tentam derrubar decreto de Bolsonaro que cria cadastro base do cidadão. **Folha de São Paulo**. 2019. Disponível em: <https://www1.folha.uol.com.br/tec/2019/10/deputados-tentam-derrubar-decreto-de-bolsonaro-que-cria-cadastro-do-cidadao.shtml>. Acesso em: 29 nov. 2019.

319 GAVIOLI, Alan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. **Infomoney**. 2019. Disponível em: <https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/>. Acesso em: 29 nov. 2019.

320 DOSHI, Vidhi. A security breach in India has left a billion people at risk of identity theft. **Washington Post**. Disponível em: <https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?noredirect=on>. Acesso em: 15 mar. 2019.

to, revela-se. Imagine-se a possibilidade de vazamento desses cadastros biométricos brasileiros que contivessem a forma de andar, ou ainda, a forma de segurar um celular?

Já foi noticiado por diversas vezes a utilização inadequada de dados dos cidadãos detidos pelo Poder Público no Brasil, como o oferecimento pelo prefeito de São Paulo de dados do Bilhete Único à iniciativa privada,[321] aplicativos de *e-gov* que não se alinham sequer ao consentimento e coletam mais do que o necessário,[322] suspeita de venda de dados pelo *Serpro*,[323] entre outros casos.

Danilo Doneda (2006, p. 401) já aduzia que:

> O escopo da tutela a qual visa este órgão supõe uma neutralidade frente às próprias razões de Estado, que seria inatingível sem esta independência. Note-se que o Estado, – e, em particular, o poder executivo – apresenta demasiado interesse na coleta e processamento de dados pessoais para que esta sua atividade possa harmonizar-se com a proteção destes mesmos dados, ao menos com a isenção necessária.

Também, para Stefano Rodotà (2008, p. 86), a independência da Autoridade de Proteção de Dados deve ser assegurada principalmente em relação ao Poder Executivo, pois entre as funções mais delicadas de controle estão em intervir em bancos de dados diretamente ligados com a ação estatal.

Assim, há um dilema no tratamento de dados pelo Poder Público, já

321 LEMOS, Ronaldo. Proposta de Doria de vender os dados do Bilhete Único é ilegal. Folha de São Paulo. São Paulo, fevereiro 2017. Disponível em: <https://www1.folha.uol.com.br/colunas/ro naldolemos/2017/02/18 60214-proposta-de-doria-de-vender-os-dados-do-bilhete-unico-e-ilegal.shtml> Acesso em: 24 nov. 2019.

322 ABREU, Jacqueline; LAGO, Lucas e MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais? **Internetlab**. São Paulo, maio 2018. Disponível em: <http://www.internet lab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/>. Acesso em: 24 nov. 2019.

323 DELGADO, Márcia. Serpro é suspeito de vender dados pessoais para administração pública. **Metrópoles**. Distrito Federal, maio 2018. Disponível em: <https://www.metropoles.com/distrito-federal/serpro-e-suspeito-de-vender-dados-pessoais-para-administracao-publica>. Acesso em: 24 nov. 2019.

que entre os pontos positivos do tratamento desses dados estão a criação de políticas públicas baseadas em evidências; a melhoria na eficiência e consequentemente desburocratização do serviço público e o desenvolvimento de inovação no governo.

A necessidade de um governo movido a dados se faz cada vez mais presente e o Governo federal vem se alinhando a ser mais digitalizado, como se vê pelo o estabelecimento de "Estratégia de Governança Digital"[324] e da análise da OCDE do "Governo Digital no Brasil".[325]

Por outro lado, existem grandes riscos como o cruzamento de bases de dados públicas formadas em contextos distintos, como a formação de perfis biométricos e comportamentais; o compartilhamento proposital, ou não, com o setor privado e os riscos de segurança cibernética. Já que a relação cidadão-Estado é formada pelo pacto social, o Estado estaria sujeito a obrigações mais elevadas de transparência.

O Estado na LGPD é tratado de diversas formas: administração pública,[326] pessoa jurídica de direito público,[327] poder público[328] e entidades públicas.[329] Aparenta-se uma leve confusão entre os conceitos anteriores que não necessariamente abrangem as mesmas competências.

Como exemplo está no art. 23[330] da LGPD que discorre sobre o tra-

---

324 BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. **Estratégia de Governança Digital: Transformação Digital – cidadania e governo**. Brasília: MP, 2018. Disponível em: <https://www.governodigital.gov.br/EGD/documentos/revisao-da-estrategia-de-governanca-digital-2016-2019.pdf> Acesso em: 25 nov. 2019.

325 ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO – OCDE. Digital Government Review of Brazil. **OECD Digital Government Studies**, [s.l.]. p.1-146, 28 nov. 2018. OECD. http://dx.doi.org/10.1787/9789264307636-en. Disponível em: <http://www.oecd.org/governance/digital-government-review-of-brazil-9789264307636-en.htm>. Acesso em: 6 nov. 2019.

326 Art. 5º (órgão de pesquisa), Art. 7º e Art. 11.

327 Art. 3º, Art. 4º, § 2º, Art. 23, Art. 27 e Art. 33, parágrafo único.

328 Art. 4º, § 4º, Art. 23, §§ 3º e 4º, Art. 26, Art. 29 e Art. 32.

329 Art. 5º, XVI; Art. 11, § 2º, Art. 26, Art. 31 (órgãos públicos), Art. 33 e Art. 52, § 3º.

330 Art. 23. O tratamento de dados pessoais pelas **pessoas jurídicas de direito público** referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as

tamento de dados pessoais pelas pessoas jurídicas de direito público, citando diretamente que estas pessoas serão as referidas no parágrafo único[331] do art. 1º da Lei de Acesso à Informação (Lei n. 12.527/2011). Contudo, neste parágrafo único são citadas diversas pessoas jurídicas de direito privado, como fundações públicas, empresas públicas e sociedades de economia mista. Assim, deve haver um esforço interpretativo para analisar cada situação citada pela legislação.

Este Estado amplamente citado deve alinhar seus clássicos princípios como o princípio da impessoalidade, da moralidade e da publicidade, com os novos princípios elencados na legislação, como o princípio da finalidade,[332] da necessidade[333] e da adequação[334] dos usos dos dados. Destaque-se, ainda, que algumas sanções instituídas pela legislação são aplicáveis aplicado às entidades e aos órgãos públicos.

Questão sensível no tocante à Autoridade foram as sanções administrativas impostas pela legislação em seu art. 52,[335] principalmente do

competências legais ou cumprir as atribuições legais do serviço público, desde que: [...] (grifos nossos)

331 Parágrafo único. Subordinam-se ao regime desta Lei: I – os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II – as autarquias, **as fundações públicas, as empresas públicas, as sociedades de economia mista** e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. [...]

332 Os dados devem ser tratados de acordo com a finalidade para a qual foram coletados inicialmente.

333 Os dados não devem ser tratados para além daquilo necessário para alcançar a finalidade almejada.

334 Os dados devem ser tratados de maneira apropriada ao contexto que justificou sua coleta.

335 Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I – advertência, com indicação de prazo para adoção de medidas corretivas; II – multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III – multa diária, observado o limite total a que se refere o inciso II; IV – publicização da infração após devidamente apurada e confirmada a sua ocorrência; V – bloqueio dos dados pessoais a que se refere a infração

seu inciso II, que prevê multa simples de até 2% do faturamento da empresa ou grupo, limitada à R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Tal disposição que tornou a LGPD tão conhecida nos meios midiáticos,[336] geralmente não é analisada contextualmente. Para que uma multa de até 2% chegue à cifra supracitada, o faturamento da empresa, excluídos os impostos, deve ser de R$ 2 bilhões e 500 milhões de reais, o que não é a realidade da maioria das empresas brasileiras.

Em verdade, a previsão dessa multa se alinha à presença de poucas *big techs* dominantes e que objetivam ser monopolistas na atuação na rede. Ademais, a aplicação de uma multa desse porte certamente ocorreria após reiteradas ocorrências e aplicação de sanções mais leves, já que esta necessidade está concretamente positivada no §1º do art. 52.[337]

O argumento de que o custo de conformidade é elevado também

até a sua regularização; VI – eliminação dos dados pessoais a que se refere a infração; VII – (VETADO); VIII – (VETADO); IX – (VETADO). X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

336 Como exemplos, Cf.: SILVA, Rafael. Multa de R$ 50 milhões será aplicada às empresas que não se adequarem à LGPD. **Canal Tech**. Disponível em: <https://canaltech.com.br/legislacao/multa-de-r-50-milhoes-sera-aplicada-as-empresas-que-nao-se-adequarem-a-lgpd-124552/>. Acesso em: 25 nov. 2019; LOBO, Ana Paula. LGPD: multa vai doer apenas no bolso de empresa brasileira. **Convergência Digital**. Disponível em: <https://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=51554&sid=4>. Acesso em: 25 nov. 2019

337 § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios: I – a gravidade e a natureza das infrações e dos direitos pessoais afetados; II – a boa-fé do infrator; III – a vantagem auferida ou pretendida pelo infrator; IV – a condição econômica do infrator; V – a reincidência; VI – o grau do dano; VII – a cooperação do infrator; VIII – a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX – a adoção de política de boas práticas e governança; X – a pronta adoção de medidas corretivas; e XI – a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

não deve se sustentar, pois é uma tendência global que empresas alinhadas com a política internacional estejam adaptadas às regras de proteção de dados pessoais.

Em um país com uma cultura de proteção de dados pessoais a ser desenvolvida, sanções como a publicização da infração, por vezes, podem obter um efeito corretivo e educacional mais adequado do que efetivamente obrigar ao pagamento de multas. Quem porventura causar danos deve se responsabilizar por eles mesmo que de maneira não pecuniária.

Assim, os objetivos das sanções na LGPD não envolvem tão somente a reparação dos danos ocasionados, mas também aspectos preventivos para propriamente se evitar a ocorrência de novos danos no futuro.

O art. 52 foi alvo de vetos tanto no momento do primeiro sancionamento da Lei Geral, quanto no momento do sancionamento da Medida Provisória convertida na Lei n. 13.853/2019. Quando do sancionamento desta, vetaram-se ainda os dispositivos dos incisos:

> X – suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI – suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Como argumento dos vetos estava a possibilidade de gerar insegurança àqueles que tratam os dados, podendo gerar prejuízo ao sistema financeiro nacional e prejuízo a entes públicos, afetando o funcionamento destes. No entanto, estes vetos foram derrubados pela maioria absoluta do Congresso Nacional.[338]

*É estabelecido no a*rt. 55-K que a aplicação das sanções previstas na lei compete exclusivamente à ANPD e suas competências prevalecerão

338 BRASIL. Congresso Nacional. **Veto n. 24/2019 (Proteção de dados pessoais)**. Disponível em: <http://tiny.cc/bbeugz> Acesso em: 25 nov. 2019.

sobre as competências correlatas de outras entidades ou órgãos da administração pública, quando o tema for a proteção de dados pessoais.

Contudo, a ANPD poderá articular sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, contudo, permanecendo aquela o órgão central de interpretação da LGPD.

Assim, há a construção de uma tese de cooperação institucional, como a essencial cooperação entre a Secretaria Nacional do Consumidor (SENACON) e a ANPD, já que no Brasil, diferentemente de outros países cujo modelo de proteção de dados foi inspirado, há uma estrutura muito robusta de defesa do consumidor e direitos difusos com alta penetração no Ministério Público[339] quanto no Poder Judiciário.[340]

A Lei Geral de Proteção de Dados Pessoais surge em um contexto internacional de ampla evolução da discussão de proteção de dados pessoais, enquanto, no Brasil, o tema é consideravelmente novo e implica um processo de conformidade tanto das empresas privadas, quanto do setor público.

Os dois anos[341] de *vacatio legis* da lei podem não ser tempo hábil para uma transição de cultural de proteção de dados pessoais que atinjam tanto as empresas quanto os consumidores. A instalação da ANPD, também, que poderia desde já estar regulamentando a lei, torna a situação mais sensível, pois a autoridade é ponto vital para que a legislação possua aplicabilidade prática e coloque o País nos moldes internacionais de proteção.

339 Em novembro de 2017, o Ministério Público do Distrito Federal criou Comissão de Proteção dos Dados Pessoais. A instituição revela-se preocupada com a proteção de dados também em outros estados, como exemplo do Ministério Público do Rio de Janeiro na ação contra a Decolar.com, citada no subitem 3.3.2.

340 O regime de proteção de dados, no Brasil, tem se destacado por meio de proposições de ações que se baseiam na proteção do consumidor. Como exemplo está a ação do IDEC contra a concessionária da Linha 4 do metrô de São Paulo, que para o deferimento de tutela de urgência utilizou-se de critérios consumeristas e dos parâmetros de abusividade já consolidados no STJ.

341 Inicialmente, a LGPD entraria em vigor decorridos 18 meses da publicação. Após, com a Medida Provisória 869/2018, ratificada pela Lei n. 13.853/2019, o prazo foi alargado para 24 meses. Contudo, há movimentações na Câmara dos Deputados que pretendem alargar ainda mais este prazo, como o Projeto de Lei n. 5762/2019 proposto em 30 de outubro de 2019. De acordo com o Projeto, caso aprovado, a *vacatio legis* da LGPD findaria apenas em 2022, vigorando a legislação em 15 de agosto de 2022.

4.5 Bases legais para tratamento de dados pessoais: tentativa de mudança da centralidade do consentimento

A atividade de tratamento de dados pessoais se verifica nas mais variadas atividades no mundo *on-line* ou *off-line*. Desde a coleta ao descarte dos dados, incluindo um mero armazenamento, para a definição legal se está realizando tratamento de dados pessoais.

Mais precisamente, para o art. 5º, X da LGPD tratamento é:

> toda operação realizada com dados pessoais, como as que se referem a **coleta**, produção, recepção, classificação, utilização, acesso, reprodução, **transmissão**, distribuição, processamento, arquivamento, **armazenamento**, **eliminação**, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (grifos nossos)

Convencionou-se chamar de "bases legais para tratamento de dados pessoais" as hipóteses em que o tratamento poderia ocorrer. O termo "bases legais" popularizou-se pela análise das hipóteses estabelecidas pelo RGPD, contudo não é em momento algum citado no regulamento ou na LGPD. Por exemplo, a autoridade britânica *Ico.* denomina as hipóteses de tratamento como *Lawful Basis for Processing*.

O RGPD europeu elencou seis bases legais de autorização de tratamento de dados pessoais no art. 6º[342]: "consentimento, execução contra-

342 Art. 6º Licitude do tratamento 1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção

tual, cumprimento de obrigação jurídica, defesa de interesses vitais do titular, necessidade para o exercício de funções de interesse público e para efeito dos interesses legítimos".

Partindo da inspiração europeia, indicaram-se dez bases de tratamento na LGPD, que abrangem as anteriores, acrescidas de bases peculiares ao regime jurídico brasileiro. Estas bases legais independem do consentimento para a sua completa validade, bem como é inexistente hierarquia entre elas, podendo o controlador utilizar-se da mais adequada ou, se preferir, múltiplas bases legais.

No art. 11 da legislação foram especialmente destacadas as hipóteses de tratamento de dados pessoais sensíveis que se regem basicamente em dois subgrupos: aquele tratamento com consentimento específico e destacado e o tratamento sem consentimento, mas desde que se enquadre nas hipóteses em que for indispensável, que são comparativamente similares as bases legais amplas de tratamento de dados pessoais. As bases de dados pessoais e dados pessoais sensíveis serão tratadas a seguir, de forma conjunta.

A primeira base legal brasileira é o **consentimento**. Esta base legal, amplamente discutida no primeiro capítulo, ainda possui um inegável peso na proteção de dados pessoais, refletindo isto na novel lei brasileira. A figura do consentimento coloca o usuário em inegável posição de responsabilidade sobre a disposição dos próprios dados, quando, em verdade, muitas vezes sequer sabe das consequências do compartilhamento.

Para Bruno Bioni (2019, p. 117), o progresso geracional da proteção de dados pessoais não eliminou o protagonismo do consentimento, já que, em vez, faz o titular dos dados pessoais permanecer na posição central de emitir a sua vontade sobre o tratamento. O autor afirma que "Mais uma vez, portanto, o consentimento avoca para si o papel de protagonista, sendo, inclusive, um dos fios condutores da recente reforma (regulação) da diretiva europeia de proteção de dados pessoais".

O Marco Civil da Internet já adotava, em 2014, parâmetros de consen-

dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

timento do titular, como o exemplo do seu art. 16, II, que informa que é vedada a guarda "de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular". Em ambas as consultas públicas realizadas pelo Ministério da Justiça, tanto em 2010 quanto em 2015, o consentimento era a única base legal de tratamento, estando no *caput* do art. 7º do anteprojeto que aduzia: "O tratamento de dados pessoais somente é permitido após o consentimento livre, expresso, específico e informado do titular, salvo o disposto no art. 11".

Quanto aos dados pessoais sensíveis, o art. 11 estabeleceu em seu primeiro inciso a possibilidade de tratamento pelo consentimento quando "[...] o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas". Dessa forma, caso o consentimento seja coletado *on-line*, a arquitetura de rede deverá ser especialmente modificada de forma a atingir essa especificidade do consentimento em cada finalidade de tratamento de dados pessoais sensíveis. Com isso, os atuais modelos de termos de uso não se prestam a coletar sequer o consentimento de dados pessoais, imagine-se o consentimento de dados pessoais sensíveis.

Ainda, como será visto na terceira base legal, as hipóteses de tratamento pelo Poder Público foram especialmente reduzidas. Assim, o Estado poderia, em tese, utilizar-se de outras bases legais para justificar o tratamento de dados pessoais. Contudo, aparentemente, o consentimento não seria uma base legal aplicável.

Entre as qualificadoras do consentimento estão a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais. Contudo, um cidadão poderia não consentir que seu dado seja tratado pelo Estado? Neste caso, não haveria no que se falar em consentimento, já que há uma relação de hierarquia do Poder Público, relação altamente assimétrica de poderes, não existindo a possibilidade de consentir pelo próprio pacto social.

Quando há uma relação muito assimétrica de poderes, há uma grande dificuldade de acusar o consentimento como realmente livre. Contudo, existem possibilidades que o Estado se relaciona com os cidadãos de maneira essencialmente informal e voluntária, como é o caso de aplicativos de governo digital ou a utilização de *wi-fi* público. Nesses casos em que a

relação deixa de ser essencialmente assimétrica e o consentimento pode ser dado de forma livre, como a possibilidade de escolher se conectar à rede pública de internet, o consentimento poderia ser, nesses restritos casos, uma base legal legítima para tratamento de dados do titular.

Outra questão sensível em relação ao tratamento de dados pessoais pelo consentimento é a possibilidade de revogação pelo titular a qualquer momento.[343] Ao revogar o consentimento, é retirado do controlador a possibilidade de tratar aqueles dados consentidos, incluindo neste tratamento, destaque-se, o mero armazenamento. Com isso, a atividade de tratamento partindo do consentimento restou seriamente fragilizada. Apesar disto, a LGPD dedica diversos artigos[344] ao consentimento como se este ainda fosse o aspecto determinante do tratamento de dados pessoais.

Assim, percebe-se o quão saudável foi a intensa discussão legislativa que culminou em diversas bases legais que não necessariamente se filiam à corrente do consentimento. Afinal, no mundo hiperconectado, pedir ao usuário um consentimento inequívoco a cada passo na rede virtual torna o instituto cada vez mais falho.

A instituição de novas bases legais revela uma busca por modelos de tratamento de dados menos fictícios e mais alinhados com as expectativas dos titulares. Cabe à ANPD a regulamentação das bases legais de formas que elas se tornem formas reais de tratamento de dados, sem possibilidade de causar prejuízos ao controlador diligente e cauteloso.

A segunda base legal é aquela utilizada para o **cumprimento de obrigação legal ou regulatória pelo controlador**. Essa hipótese está igualmente apresentada para o tratamento de dados sensíveis na alínea a) do art. 11, II: "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II – sem fornecimento de con-

343 LGPD, Art. 8º, § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

344 Art. 5º, XII; Art. 7º, I, §§ 4º, 5º, 6º; Art. 8º, §§1º, 2º, 3º, 4º, 5º, 6º; Art. 9º, §§1º , 2º; Art. 11, II, §2º; Art. 14, §§1º, 3º, 5º; Art. 15, III; Art. 18, VI, VII, VIII, IX, §2º; Art. 19, §3º; Art. 27, I; Art. 33, VIII.

sentimento do titular, nas hipóteses em que for indispensável para: [...] a) cumprimento de obrigação legal ou regulatória pelo controlador".

Como exemplo desta operação está o setor financeiro, que tem a obrigação de guardar as informações dos clientes, consoante a Circular n. 3.461/2009[345] do Banco Central. Ou até mesmo um empregador que necessita recolher impostos de seus empregados carece, assim, manter dados sobre eles. Ademais, o Poder Público poderia evocar essa base legal a partir do princípio da legalidade em casos que não fossem diretamente aplicáveis a terceira base legal, que é especialmente direcionado a esta entidade.

Neste caso, não há qualquer intervenção do titular dos dados, contudo, em virtude da autodeterminação informativa prevista na lei, o controlador deverá informar que os dados serão recolhidos sem o consentimento, justificando a base legal de tratamento.

Todavia, a diferenciação do tratamento para se cumprir uma obrigação legal é utilizar os dados essencialmente para o objetivo previsto desta obrigação legal ou regulatória. Com isso, não é porque os dados foram obtidos por essa maneira que eles restam desimpedidos para serem tratados para outras finalidades. Um único banco de dados que tenha sido construído a partir de diversas bases legais – uns pelo consentimento, outros por cumprimento de obrigação legal – deve ser o tratamento justificado e enquadrado de acordo com cada base legal apropriada.

A terceira base legal é aquela prevista para a administração pública, com fins de tratamento e uso compartilhado de dados necessários à **execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres**. No caso de tratamento de dados pessoais sensíveis, as hipóteses são reduzidas apenas à execução de políticas públicas previstas em leis e regulamentos.

Esta base legal é especialmente direcionada à administração pública, contudo, quando se delimitam apenas essas hipóteses, percebe-se que outras atividades de tratamento de dados pelo Estado foram excluídas. Por exemplo, o pagamento de servidores públicos, as atividades de

345 BRASIL. Banco Central do Brasil. **Circular n. 3.461 de 24/7/2009**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3461> Acesso em: 26 nov. 2019.

poder de polícia administrativa, o repasse de recursos, entre outras hipóteses que não estão expressamente excluídas no art. 4º da LGPD[346], mas também sequer foram citadas como uma hipótese de tratamento.

Assim, quando o caput do art. 7º[347] insere a palavra "somente" e o inciso terceiro insere apenas a hipótese para execução de políticas públicas, olvida o legislador que o Poder Público não faz somente política pública. Essas hipóteses sequer são suficientes para abarcar todas as atividades do Poder Público.

Com isso, para superar essa dificuldade interpretativa que a palavra "somente" inseriu no art. 7º, é necessária uma leitura sistemática e conjugada com o art. 23 da LGPD que aduz:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as **competências legais ou cumprir as atribuições legais do serviço público**, desde que: se atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> II – (VETADO); e

346 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II – realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

347 Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.

> III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei.
> III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e
> IV – (VETADO) (grifos nossos).

Assim, essa leitura conjugada fornece parâmetros mais amplos para atender às hipóteses em que o Poder Público em seu sentido mais amplo pode tratar dados pessoais.

A base legal de número quatro é aquela para a realização de **estudos por órgão de pesquisa, garantida**, sempre que possível, a anonimização dos dados pessoais. A LGPD preocupou-se em estabelecer essa base legal, bem como destacar critérios em que estes órgãos deverão proteger os dados pessoais e dados pessoais sensíveis. É neste contexto que a legislação cita que deverá ocorrer, sempre que possível, a anonimização e a pseudonimização dos dados.[348]

A quinta base legal é aquela que é necessária para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

A situação para execução de contratos talvez seja a base legal que mais possa se adequar nas atividades cotidiana de uma empresa de serviços, desde uma agência de turismo *on-line*, até a utilização dos dados da reserva por um hotel para operacionalizar a hospedagem.

Esta base legal assemelha-se à hipótese de cumprimento de obrigação legal ou regulatória pelo controlador, só que, em vez, a obrigação será contratual. Com isso, o titular dos dados deverá ter previamente consentido e assinado um contrato com o controlador e, para a necessária execução deste, é indispensável o tratamento dos dados pessoais.

Contudo, não se deve tratar nesta base legal dados que seriam inúteis à atividade empresarial de tratamento. De acordo com o *Ico.*, ao explicar esta base legal, aduz que a execução contratual deve ser um passado

348 Quanto isto, remonta-se a questão sobre a real possibilidade de anonimização de dados discutida no subitem 4.3.

direcionado e proporcional para entregar o serviço ou ação ao indivíduo. Esta base legal não deverá ser aplicada se existirem outros meios mais razoáveis ou menos intrusivos de fornecer o serviço solicitado.[349]

A base legal elencada no inciso VI se verifica para os casos de **exercício regular de direitos em processo judicial, administrativo ou arbitral.** Este caso não é apenas aplicável ao Estado enquanto Poder Judiciário, já que utilização de bancos de dados pelo Poder Judiciário estão abrangidas em hipóteses de cumprimento de obrigação legal.

Em verdade, trata-se de permitir que uma das partes envolvidas em um litígio não tenha os seus preceitos constitucionais da ampla defesa e do contraditório cerceados por questões de tratamento de dados pessoais. Assim, trata-se de uma base legal para garantir o direito de produção de provas de uma parte contra a outra em um processo judicial, administrativo ou arbitral.

A sétima base legal é para a **proteção da vida ou da incolumidade física do titular ou de terceiros.** Esta base também pode ser extraída do regulamento europeu, em que está disposta como: "O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;".

A razão de inserção desta base no regramento europeu teve em vista as transferências por organizações humanitárias com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados. De acordo com o considerando 46 do GDPR: "[...] o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico". Entre os exemplos elencados no regulamento está não somente a utilização por fins humanitários, mas também o monitoramento de epidemias e emergências humanitárias, como catástrofes naturais e de origem humana.

A oitava base legal abrange a **tutela da saúde, exclusivamente, em**

349 INFORMATION COMMISSIONER'S OFFICE. *Lawful basis for processing.* 2019. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> Acesso em: 29 nov. 2019.

procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Esta poderia se enquadrar em mais uma hipótese de tratamento para o Poder Público, mas pode aplicar-se também ao setor privado.

Pretende-se nesta incluir aspectos próprios ao regime de saúde pública no Brasil, contudo, essa base legal está intimamente relacionada com a base legal anterior que foi extraída diretamente do regulamento europeu. Inclusive, a autoridade inglesa ao citar hipóteses de aplicação da base legal de proteção de interesses vitais, cita um exemplo que seria aplicável à base legal brasileira: "Um indivíduo é internado no departamento de acidentes e emergências de um hospital com ferimentos graves após um sério acidente de rodovia. A divulgação ao hospital do histórico médico do indivíduo é necessária para proteger seus interesses vitais".[350]

A penúltima situação de tratamento de dados pessoais é aquela quando necessária para atender aos **interesses legítimos** do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. Esta base legal não é cabível para tratamento de dados sensíveis.

Essa base legal, que se tornou mais conhecida como "legítimo interesse", em uma simples leitura do inciso pode parecer uma carta branca do legislador em relação às demais bases. Contudo, se não forem tomadas as devidas precauções, pode ser alta fonte de responsabilizações futuras. Assim, entre outras exigências, o controlador diligente deverá elaborar relatório de impacto à proteção de dados pessoais que poderá ser solicitado pela ANPD.

Esta base legal é melhor disposta no art. 10 da LGPD, que dispõe que para o tratamento devem existir finalidades legítimas, que podem incluir o apoio e promoção de atividades do controlador ou a proteção do exer-

350 Tradução livre: "*An individual is admitted to the A&E department of a hospital with life-threatening injuries following a serious road accident. The disclosure to the hospital of the individual's medical history is necessary in order to protect his/her vital interests*". INFORMATION COMMISSIONER'S OFFICE. **Lawful basis for processing**. 2019. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>. Acesso em: 29 nov. 2019.

cício regular de seus direitos ou prestação de serviços que beneficiem o titular dos dados.

O legítimo interesse pode ser melhor exemplificado como um teste de ponderação realizado pelas empresas sobre a necessidade de utilização dos dados e a existência de finalidade legítima e propósito específico. Vale ressaltar que a base legal trata do interesse legítimo da empresa em tratar certos dados, devendo este ser provado por meio de Relatório de Impacto à Proteção de Dados – RIPD (*Data Protection Impact Assessment* – DPIA).

O relatório de impacto, na definição do art. 5º, XVII, é a documentação do controlador "que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco". Este documento seria um sistema de pesos e contrapesos para que o legítimo interesse não vire um cheque em branco.

Na lógica brasileira, a exigência do relatório de impacto poderá ser feita ou não, após a realização do tratamento dos dados. Contudo, a prática estrangeira revela que as empresas que optem pelo legítimo interesse deverão desde já documentar suas intenções no relatório, antes mesmo dele ser solicitado. Já no art. 38 da LGPD, que não necessariamente se refere ao tratamento de dados pela base legal do legítimo interesse, a autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais.

Com isso, entende-se que, no caso de tratamento de dados pelo legítimo interesse, como é uma base legal que pode aparentar ser mais permissiva, o relatório de impacto deve ser desde logo preparado, antes mesmo de uma futura requisição da autoridade. Assim, a maneira de tratar dados a partir do legítimo interesse é realizando uma documentação do uso dos dados pessoais.

Assim, a ferramenta do legítimo interesse poderá ser realizada como um efetivo teste de ponderação, e que a empresa documente o processo de tratamento, indique o *software* utilizado, onde ocorrerá o armazenamento, com quais áreas da empresa os dados serão compartilhados, entre outras necessidades de documentação do ciclo de vida dos dados que variam caso a caso.

Além de um mapeamento, RIPD deve documentar que medidas de

mitigação de risco técnicas, administrativas e organizacionais serão adotadas internamente por conta da utilização dos dados pessoais.

Na importação do DPIA e sua conversão ao sistema brasileiro como RIPD, houve a inserção de situações em que o relatório de impacto não foi originalmente concebido no RGPD. Para a utilização do legítimo interesse no regulamento, em vez de um relatório de impacto, seria cobrado um *Legitimate Interests Assessment* (LIA), que é um teste de balanceamento, já que efetivamente deve-se testar em análise concreta e jurídica como a situação se aplica à base legal em comento. De acordo com o *Ico.*, o teste possui a seguinte função:

> O teste de balanceamento é onde você leva em consideração "os interesses ou direitos e liberdades fundamentais do titular dos dados que exigem a proteção de dados pessoais" e verifica se eles não substituem os seus próprios interesses. Em essência, essa é uma avaliação de risco leve para verificar se os riscos para os interesses dos indivíduos são proporcionais.[351]

Assim, o LIA é um registro desse balanceamento realizado pela empresa para definir se os dados serão legitimamente utilizados, se os dados a serem tratados serão realmente necessários e quais são os direitos dos titulares que poderiam estar em risco pela utilização dos dados pela empresa. Este registro, portanto, é consideravelmente mais simples que um completo relatório de impacto. Ao LGPD citar genericamente relatório de impacto, acredita-se que será exigido das empresas o mapeamento do ciclo de dados e formas de mitigação de riscos, bem como documentar, no mesmo relatório, as competências do teste de balanceamento.

Vale destacar que o RIPD não é um documento público; é um docu-

351 Tradução livre: "*The balancing test is where you take into account 'the interests or fundamental rights and freedoms of the data subject which require the protection of personal data', and check they don't override your interests. In essence, this is a light-touch risk assessment to check that any risks to individuals' interests are proportionate*". INFORMATION COMMISSIONER'S OFFICE. **What is the balancing test?** 2019. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> Acesso em: 27 nov. 2019.

mento interno que, eventualmente, será fiscalizado pela ANPD, mas permanece protegido pelo segredo comercial e industrial.

A utilização do legítimo interesse pelo Estado também suscita discussão, mas há casos específicos em que esta base legal poderia ser utilizada. Inclusive, esta hipótese é aventada pelo *Ico.*: "As autoridades públicas só podem se basear em interesses legítimos se estiverem processando por uma razão legítima que não seja a execução de suas tarefas como autoridade pública".[352]

Como exemplo, está mais um aplicativo de governo digital, o TáxiGov. Este, em definição do Ministério da Economia, "É o serviço de transporte de servidores e colaboradores da Administração Pública Federal em deslocamentos a trabalho com o uso de táxis, que começou a ser implementado em março de 2017".[353]

Este aplicativo precisa saber os dados de localização do usuário, o sistema operacional do celular, entre outras funções para que sua operacionalidade seja razoável. Com isso, dificilmente poderá ser aplicada a base legal do consentimento, já que é uma medida do Governo Federal para obter economia de gastos,[354] ainda, dificilmente haverá uma previsão legal e, por fim, claramente não é uma política pública. Com isso, nestas hipóteses restritas, poder-se-ia falar em legítimo interesse do Estado para a coleta de dados pessoais, restando, contudo, dúvidas sobre de quem a Autoridade Nacional poderia exigir um relatório de impacto.

Por fim, a última hipótese de tratamento de dados pessoais da LGPD é aquela para a para a **proteção do crédito.** Esta base legal possui como objetivo impedir que eventuais titulares de dados pessoais inadimplen-

352 Tradução livre: "Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority". INFORMATION COMMISSIONER'S OFFICE. **Lawful basis for processing**. 2019. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/> Acesso em: 29 nov. 2019.

353 BRASIL. Ministério da Economia. **O que é o TaxiGov**. Disponível em: <http://www.economia.gov.br/ assuntos/gestao/taxigov>. Acesso em: 28 nov. 2019.

354 BRASIL. Ministério da Economia. **O que é o TaxiGov**. Disponível em: <http://www.economia.gov.br/ assuntos/gestao/taxigov>. Acesso em: 28 nov. 2019.

tes se utilizem de seus demais direitos enquanto titulares para furtarem-se de dívidas contraídas. Assim, o titular não poderá, neste caso, pedir meramente requerer a sua exclusão. Trata-se de uma base legal brasileira redundante à base legal de cumprimento de obrigação legal ou regulatória, já que nas hipóteses de proteção do crédito lícitas já estão envolvidas hipóteses legais ou regulatórias.

Entre as principais atribuições das bases legais está o resguardo do princípio da transparência. Assim, antes[355] do processamento de dados, força-se a todos aqueles envolvidos na ampla atividade de tratamento a focar as atenções nas bases legais especificadas pela lei.

Muitas delas ainda serão melhor explicadas e abrangidas pela regulamentação da ANPD, contudo, a partir do vigor da LGPD, será preciso observar a lógica de proteção de dados pessoais estabelecida, bem como buscar contínuo alinhamento com as legítimas expectativas do usuário.

355 Ou depois, como no caso de proteção da vida do titular dos dados pessoais.

5 Considerações finais

A partir dos tópicos debatidos no trabalho, percebe-se que as técnicas de monitoramento do usuário são parte essencial da movimentação econômica e personalização da experiência *on-line*, com reflexos na capacidade de decisão e de escolha do cidadão.

O capítulo inicial, além de destacar os reinados tecnológicos invisíveis das *big techs*, bem como a sua inserção em uma sociedade de vigilância, analisou a evolução do direito à privacidade, que partiu da perspectiva individualista para a inclusão de novos interesses, de forma que o balanço constitucional esteja correto e a fundamentalidade da intimidade e da vida privada estejam efetivamente protegidas.

A partir da pergunta "Quais são as novas feições do direito à privacidade relacionadas ao eixo constitucional da proteção da pessoa?", apresentou-se que os estudos

do direito à privacidade evoluíram ao ponto desse direito apresentar ramificação mais pertinente à matéria da proteção de dados pessoais, o direito **à autodeterminação** informativa. Esse direito, criado a partir de decisão da Corte Constitucional Alemã, é amplamente defendido em matéria de proteção de dados pessoais como o direito do titular de conhecer e controlar as informações que circulam sobre sua pessoa.

Ainda no capítulo 2, passou-se à análise do consentimento e a sua evolução ao pseudoconsentimento com a abordagem da interrogativa: quais são os desdobramentos do consentimento no ambiente digital? Para a Lei Geral, o consentimento deve ser livre, informado, inequívoco e com finalidade determinada. Contudo, a situação se torna nebulosa quando trata dos hipervulneráveis, pois estes não teriam capacidade jurídica para consentir. Apesar da possibilidade de ser externado consentimento nestes casos pelo responsável legal, tal solução não se revela prática aos rápidos hábitos modernos e, ao mesmo tempo, não se deveria regredir na digitalização e na virtualização consciente de crianças e adolescentes, sob pena de causar uma evidente exclusão social no círculo de convivência destas.

As interações digitais cada vez mais se resumem em cliques e duplos cliques que ressaltam a difícil compreensão da carga informacional do que se está clicando ou concordando. Tradicionalmente, a obtenção do consentimento se dá pelos rápidos cliques após descer a barra de rolamento de um contrato.

O alcance jurídico abusivo de um clique na cláusula "Li e Aceito" não deve permanecer, pois diversas pesquisas referenciadas no item 2.4.5 atestaram que os usuários passam menos de um minuto para ler longos contratos ou sequer fazem contato visual com a integralidade do arquivo.

Assim, também se conclui, no capítulo 2, que há a necessidade de melhor estruturação da arquitetura de rede, já que, sem a devida facilitação da compreensão do conteúdo, as cláusulas de "Li e Aceito" são revestidas de um pseudoconsentimento.

No segundo capítulo chega-se à conclusão, ainda, que há um paradoxo da personalização, em que a tecnologia capaz de capturar e estratificar os dados pessoais dos usuários é capaz também de ser personalizada para melhoramento de diversos aspectos da vida humana, contudo, contraditoriamente, os contratos vinculados a tais tecnologias permitem ne-

nhuma ou uma mínima personalização a cada usuário.

A utilização de *Privacy Enhancing Technologies* (PETs) deve ser estimulada para que se desenvolvam a ponto de que se apresentem como ferramentas viáveis a serem aplicadas para a proteção dos dados pessoais e para que, principalmente, possuam plena executoriedade pela *World Wide Web Consortium* (W3C), organização de padronização da internet.

No terceiro capítulo buscou-se mapear as práticas mais comuns de coleta de dados para publicidade comportamental, como forma de atentar-se à pergunta: quais são as práticas mais comuns e as consequências da sua utilização para obtenção de dados para direcionamento de publicidade nos novos modelos de comércio eletrônico? Entre as mais referenciadas na literatura estão o *profiling* e o *machine learning*, as quais partem de suas principais ferramentas – como *cookies*, *web beacons*, *supercookies,* HTML5 *web storage* e *fingerprinting*.

Ademais, estudou-se as variadas composições da definição de *big data*, que é uma inovadora metodologia de estruturação de dados. Não é um sistema inteligente, mas, por partir de seu imenso volume, é capaz de fornecer correlações acuradas para as propostas lançadas em seu sistema.

Entre as pretensões do *big data* está a realização de correlações entre os dados e as estatísticas as quais buscam encontrar. Essas correlações são alcançadas a partir de uma análise de dados que, por meio das ferramentas de rastreio do usuário, coletam os mais variados dados sobre certo indivíduo.

Concluiu-se neste capítulo que a interação entre o *big data* e a publicidade comportamental geram a modelagem comportamental *on-line*. Esta, que se funda na criação de algoritmos para realizar correlações em *big data analytics*, pode envolver em risco à privacidade, risco de viés, risco ao erro e risco de exploração aos usuários.

Estes riscos estão inseridos na utilização cotidiana de sistemas automatizados que não necessariamente possuem uma transparência no processo decisório e, mesmo que essa transparência exista, não significa que as decisões por ele tomadas serão legítimas.

No capítulo 3, realizou-se análise de casos e situações paradigmáticas que envolveram grandes riscos de manipulação de dados por *profiling*, bem como riscos de exploração e à privacidade dos usuários. Entre os

casos, analisou-se a suposta descoberta pela empresa *Target* da gravidez de uma adolescente por meio de *big data analytics*; a realização de práticas de *geopricing* e *geoblocking* pela empresa Decolar.com, em detrimento de consumidores brasileiros; a coleta de reações de usuários pela concessionária da Linha 4 Amarela do metrô de São Paulo, para análise de desempenho de publicidades mostradas aos passageiros; e, por fim, questões de privacidade e de gênero que permeiam a utilização constante de assistentes pessoais virtuais no dia a dia.

Diagnosticado esse cenário, passou-se a analisar, no capítulo 4, as perspectivas do tratamento legal de dados pessoais no Brasil na Lei Geral de Proteção de Dados n. 13.709, de 14 de agosto de 2018, verificando suas condições de encerrar o país em patamares internacionais quanto à proteção de dados.

Com isso, este capítulo partiu das perguntas: uma estrutura jurídica de proteção europeia serve aos propósitos brasileiros? Qual a importância da revisão humana de decisões automatizadas? A Autoridade Nacional de Proteção de Dados possuirá funcionalidade para proteção dos consumidores? Ainda há um superdimensionamento do consentimento em detrimento das demais bases legais de tratamento de dados pessoais?

Iniciou-se traçando o histórico de inspiração, surgimento e elaboração da LGPD, bem como as dificuldades legislativas enfrentadas para a evolução da redação legal. Esta, que inicialmente era dominada pela figura do consentimento, foi posteriormente balanceada com alterações que pretendem fornecer novas bases legais de análise de tratamento de dados pessoais.

A LGPD possui inegável influência europeia, apesar das formações sociais de brasileiros e europeus serem bastante distintas, já possuindo a doutrina europeia de proteção de dados pessoais desenvolvido desde 1980 os *Fair Information Practice Principles* (FIPPs).

Neste sentido, a simples promulgação de uma lei de proteção de dados brasileira não significa automático reconhecimento de equivalência para ocorrer transferência internacionais entre brasileiros e europeus. A ausência de instalação de uma autoridade independente também é aspecto prejudicial ao posicionamento brasileiro em transferências internacionais de dados pessoais.

A existência de dispositivo que elencava a necessidade de revisão

humana de decisões automatizadas e, por isso, apresentava incrível avanço da legislação brasileira em relação à europeia, infelizmente foi vetado da legislação. Com isso, a situação que se concluiu no capítulo 3 permanece sem solução sobre a possibilidade de prejuízo aos cidadãos que são submetidos à uma decisão algorítmica opaca e que poderia ter sido aprimorado com o dispositivo revogado.

Além disso, a situação legal da Autoridade que ainda não foi instalada até o momento se complica, pois muitos aspectos da LGPD dependem de atuação direta da ANPD, que, a oito meses da entrada em vigência da lei, sequer está em funcionamento. Para além das sanções previstas, que foram fortemente noticiadas como um ponto negativo da LGPD, apesar de serem elas adequadas ao contexto internacional de repressão de vazamentos de dados, a Autoridade para ser efetiva deve ser capaz de regulamentar a legislação em seus pontos controversos e sensíveis, bem como assegurar a sua aplicabilidade aos operadores e controladores *on--lines* e *off-lines*.

Por fim, a LGPD inova ao abranger dez bases legais de tratamento de dados pessoais, enquanto o RGPD europeu elencou apenas seis bases legais de autorização de tratamento de dados pessoais. As bases legais da Lei Geral abrangem as anteriores, acrescidas de bases peculiares ao regime jurídico brasileiro.

Com isso, apesar de existir um superdimensionamento da lei sobre as explicações hipóteses da base legal de consentimento, há esperanças que a prática revele que o mercado, instituto capaz de se adequar mais rápido ao surgimento de tecnologias que o Direito, utilize-se de diversas bases legais para o tratamento de dados pessoais para superar, enfim, o pseudoconsentimento do usuário, tendo como motivador a não aplicabilidade das sanções previstas na Lei.

Assim, o cenário de aplicação de múltiplas bases legais torna-se viável, já que, em vez de fazer de o usuário concordar com hipóteses de tratamento de dados de A à Z por meio do consentimento, o controlador deverá elencar que, de A a G, o usuário deve consentir ou não contratar. Caso consinta, de H a V, o tratamento será realizado por existência obrigações legais, em que o controlador informa o usuário, mas não pede a sua permissão, e para realizar o tratamento de dados nas hipóteses X, Y e

Z, o tratamento ocorre como forma de execução contratual, mais uma vez previamente informada.

As limitações do presente trabalho consistem em não se ter desenvolvido com profundidade a problemática da relação do Estado com o tratamento de dados pessoais e dados pessoais sensíveis, como exemplo em operações de segurança pública, bem como as implicações de inclusão de dados biométricos e extremamente identificadores em bancos de dados públicos e privados. Entende-se que tais aprofundamentos não ocorreram por não estarem no recorte do presente trabalho, mas serem apenas desdobramentos indiretos do problema de pesquisa investigado.

Estas temáticas supracitadas revelam perspectivas futuras para o aprofundamento dos estudos do tema, sobretudo a questão da interação do Estado e cidadão-usuário, nas perspectivas cada vez mais próximas de implementação de um amplo governo digital no Brasil.

Apesar disto, o trabalho possui contribuição para a área por tratar de estudos e pesquisas empíricas estrangeiras que abordam diretamente tema de uma lei recentemente promulgada no País.

Na expressão de Danilo Doneda (2006, p. 52), "tratar de tecnologia não é *a priori* um exercício de futurologia". Com isso, é necessário que o ramo do Direito se ocupe em propriamente adequar as mudanças tecnológicas antes que estas obrigatoriamente o adequem. Deve-se sair da posição de determinismo tecnológico e da postura ingênua que tecnologia não se discute para que esta efetivamente seja meio de transformação melhoramento social.

Em um mundo em que o poder de uma grande companhia vai muito além de aumentar preços, passando em vez pelo controle da informação e de como mostrar o mundo aos usuários, a manipulação pode passar a ser não apenas dos consumidores, mas também da própria democracia.

REFERÊNCIAS

ANDERSEN, Hans Christian. *As roupas novas do imperador*. São Paulo: Ovale, 1996.

ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. 3. tiragem. São Paulo: Malheiros, 2014.

ALMEIDA, Napoleão Mendes de. *Dicionário de questões vernáculas*. São Paulo: Caminho Suave, 1981.

ASCARELLI, Tullio. *Problemas das sociedades anônimas e direito comparado*. São Paulo: Quorum, 2008.

BERGER, John. *Modos de ver.* Rio de Janeiro: Rocco, 1999.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor.* São Paulo: Almedina, 2018.

BOBBIO, Norberto. *A era dos direitos*. Rio de Janeiro: Elsevier, 2004.

BOBBIO, Norberto. *Da estrutura à função*: novos estudos de teoria do direito. Barueri: Manole, 2007.

BOFF, Salete Boro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. *Proteção de dados e privacidade:* do direito às novas tecnologias na sociedade de informação. Rio de Janeiro: Lumen Juris, 2018.

BONAVIDES, Paulo. *Curso de direito constitucional*. 30. ed. São Paulo: Malheiros, 2015.

BRANCO, Sérgio. *Memória e esquecimento na internet*. Porto Alegre: Arquipélago Editorial, 2017.

CARROLL, Lewis. *Aventuras de Alice no País das Maravilhas*. São Paulo: Editora 34, 2015.

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

CASTELLS, Manuel. *A sociedade em rede*: a era da informação: economia, sociedade e cultura. 11. ed. São Paulo: Paz e Terra, 2008. v. 1.

CASTELLS, Manuel. *Communication power*. New York: Oxford University Press, 2009.

COOLEY, Thomas. *A Treatise on the Law of Torts or the wrongs which arise independent of contract.* Chicago: Callaghan, 1879. Disponível em: https://repository.law.umich.edu/books/11/. Acesso em: 11 jun. 2019.

COMPARATO, Fábio Konder. A *afirmação histórica dos direitos humanos*. São Paulo: Saraiva, 2008.

COVELLO, Sergio Carlos. *As normas de sigilo como proteção à intimidade*. São Paulo: Editora Sejac, 1999.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. *Big Data*: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt, 2013.

CUPIS, Adriano de. *Os direitos de personalidade*. São Paulo: Quorum, 2008.

DEBORD, G. *A sociedade do espetáculo*. Rio de Janeiro: Contraponto, 1997.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar, 2006.

DUPAS, Gilberto. *Ética e Poder na Sociedade da Informação. 2*. ed. São Paulo: UNESP, 2001.

FARIAS, Edilsom Pereira de. *Colisão de direitos:* a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Sergio Antonio Fabris Editor, 2000.

FOUCAULT, Michel. *Vigiar e punir:* nascimento da prisão. 42. ed. Petrópolis: Vozes, 2014.

GIANNOTTI, Edoardo. *A tutela constitucional da intimidade.* Rio de Janeiro: Forense, 1987.

GUERRA, Sidney Cesar Silva. *O direito à privacidade na internet*: uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2004.

HAN, Byung-Chul. *No enxame.* Petrópolis: Vozes, 2018. *E-book* Google Play Livros.

HAN, Byung-Chul. *Sociedade do cansaço.* 2. ed. Petrópolis: Vozes, 2018.

KAHNEMAN, Daniel. *Rápido e devagar*: duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

KASANOFF, Bruce. *Atendimento personalizado e o limite da privacidade*: até que ponto as empresas podem usar informações pessoais para lucrar na Internet. Rio de Janeiro: Campus, 2002.

KEEN, Andrew. *Vertigem digital*: por que as redes sociais estão nos dividindo, diminuindo e desorientando. Rio de Janeiro: Zahar, 2012.

LACE, Susanne. *The glass consumer*: life in a surveillance society. Bristol: The Policy Press, 2005.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2010.

MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018. Disponível em: http://eduardomagrani.com/trilogia-trilogia-cultura-digital/. Acesso em: 23 set. 2019.

MAGRANI, Eduardo. *Entre dados e robôs*: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019, p. 48. Disponível em: http://eduardomagrani.com/trilogia-trilogia-cultura-digital/. Acesso em: 23 set. 2019.

MARMELSTEIN, George. *A judicialização da ética.* Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2018. 585 p. (Série monografias do CEJ ; 30)

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIRANDA, Leandro Alvarenga. *A proteção de dados pessoais e o paradigma da privacidade.* São Paulo: All Print Editora, 2018.

O'NEIL, Cathy. *Weapons of math destruction:* how big data increases inequality and threatens democracy. New York: Crown Publishers, 2016.

PASQUALE, Frank. *The Black Box Society:* the secret algorithms that control

money and information. Massachusetts: Harvard University Press, 2015.

POMBO, Rocha. *Dicionário de sinônimos da língua portuguesa.* Rio de Janeiro: Academia Brasileira de Letras, 2011. Disponível em: https://www.literaturabrasileira.ufsc.br/ documentos/?action=download&id=82177. Acesso em: 13 jun. 2019.

ROCHA, Everardo. *Magia e capitalismo*: um estudo antropológico da publicidade. São Paulo: Editora Brasiliense, 1990.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 14.

SANDEN. Ana Francisca Moreira de Souza. *A proteção de dados pessoais do empregado no direito brasileiro*: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. São Paulo: LTr, 2014.

SCHUMPETER, Joseph A. *Capitalism, socialism and democracy*. London: Routledge, 2003.

SCHUMPETER, Joseph A. *Teoria do desenvolvimento econômico*: uma investigação sobre lucros, capital, crédito, juro e o ciclo econômico. São Paulo: Editora Nova Cultural, 1997.

SIEGEL, Eric. *Predictive analytics*: the power to predict who will click, buy, lie, or die. New York: Wiley, 2016.

SOLOVE, Daniel. *The digital person*: technology and privacy in the information age. New York: New York University Press, 2004. p. 38. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2899131. Acesso em: 27 set. 2019.

SZIRMAI, Adam. *The dynamics of socio-economic development*: an introduction. Cambridge: Cambridge University Press, 2005.

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge:* improving decisions about health, wealth, and happiness. New York: Penguin Books, 2009.

VENTURINI, Jamila *et al. Terms of service and human rights:* an analysis of online

platform contracts. Rio de Janeiro: Revan, 2016. Disponível em: http://bibliotecadigital.fgv.br/dspace/handle/10438/18231. Acesso em: 1 maio 2019.

VIANNA, Túlio Lima. *Transparência pública, opacidade privada*: o direito como instrumento de limitação do poder na sociedade de controle. Rio de Janeiro: Revan, 2007.

WESTIN, Alan. *Privacy and freedom.* New York: Atheneum, 1967. Disponível em: https://archive.org/details/privacyfreedom00west. Acesso em: 10 abr. 2019.

WU, Tim. *The attention merchants*: the epic scramble to get inside our heads. New York: Alfred A. Knopf, 2016.

ZANON, João Carlos. *Direito à proteção dos dados pessoais.* São Paulo: Editora Revista dos Tribunais, 2013.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier power. New York: Public Affairs, 2019. Capítulo 2, tópico I, paginação irregular. *E-book* Kindle.

Capítulos de livros

BENTHAM, Jeremy. O panóptico. *In*: BENTHAM, Jeremy, TADEU, Tomaz (org.). *O panóptico.* 2. ed. Belo Horizonte: Autêntica, 2008. Disponível em: http://tiny.cc/e8jw7y. Acesso em: 6 jun. 2019.

LUCCA, Newton de. Títulos e contratos eletrônicos: O advento da informática e suas consequências para a pesquisa jurídica. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2005.

TUCCI, José Rogério Cruz e. Eficácia probatória dos contratos celebrados pela internet. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito & internet*: aspectos jurídicos relevantes. São Paulo: Quartier Latin, 2005.

Artigos e Conferências

ARAÚJO, Camila Souza; MEIRA JÚNIOR, Wagner; ALMEIDA, Virgilio. Identifying stereotypes in the online perception of physical attractiveness. *Lecture Notes in Computer Science*, Springer International Publishing, [New

York, NY], p. 419-437, 2016. Disponível em: https://arxiv.org/pdf/1608.02499.pdf. Acesso em: 4 out. 2019.

BAKOS, Yannis; MAROTTA-WURGLER, Florencia; TROSSEN, David R. Does anyone read the fine print?: testing a law and economics approach to standard form contracts. *SSRN Electronic Journal,* Amsterdam, p. 1-45, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443256. Acesso em: 30 abr. 2019.

BALEBAKO, Rebecca *et al*. Nudging users towards privacy on mobile devices. *In*: WORKSHOP ON PERSUASION, INFLUENCE, NUDGE AND COERCION THROUGH MOBILE DEVICES, 2., 2011, Vancouver, CA. *Proceedings* [...]. Vancouver, CA: CEUR, PINC at CHI-11, 2011. Disponível em: http://ceur-ws.org/Vol-722/paper6.pdf. Acesso em: 5 out. 2019.

BANERJEE, Syagnik; DHOLAKIA, Ruby Roy. Mobile advertising: does location based advertising work? *International Journal of Mobile Marketing*, New York, Dec. 2008. Disponível em: https://ssrn.com/abstract=2135087. Acesso em: 2 out. 2019.

BECKER, Gary S. A. Theory of the Allocation of Time. *The Economic Journal*, v. 75, n. 299, p. 493-517, Sept. 1965. Disponível em: http://www.jstor.org/stable/2228949. Acesso em: 20 jun. 2019.

BENTHAM, Jeremy. Da publicidade. *Revista Brasileira de Ciência Política*, Brasília, DF, n. 6, p. 277-294, dez. 2011. Disponível em: http://dx.doi.org/10.1590/S0103-33522011000200011. Acesso em: 25 set. 2019.

BIONI, Bruno. Inovar pela Lei. *GV-executivo*, São Paulo, v. 18, n. 4, jul./ago. 2019. Disponível em: https://rae.fgv.br/sites/rae.fgv.br/files/gv_0184ce5.pdf. Acesso em: 14 nov. 2019.

CABAÑAS, José; CUEVAS, Ángel; CUEVAS, Rubén. Facebook use of sensitive data for advertising in Europe. *Computer Science Cornell University,* arXiv, [Ithaka, NY], 14 fev. 2018. Disponível em: https://arxiv.org/abs/1802.05030. Acesso em: 15 nov. 19.

CARVALHO, Cristiane Mafacioli. Gênero, linguagem e estratégias do discurso publicitário da atualidade. *Revista Famecos*, Porto Alegre, v. 19, n. 32 jan. 2013, p. 821-838. Disponível em: http://dx.doi.org/10.15448/1980-

3729.2012.3.12903. Acesso em: 25 set. 2019.

CARVALHO, Victor Miguel Barros de; et al. A monetização de dados pessoais como alternativa a períodos de crise: análise jurídica a partir do marco civil da internet. *In*: *CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE: MÍDIAS E DIREITOS DA SOCIEDADE EM REDE,* 4., 2017, Santa Maria. *Anais* [...]. Santa Maria: UFSM, 2017. 17 p. Disponível em: http://coral.ufsm.br/congressodireito/anais/2017/9-2.pdf. Acesso em: 15 mar. 2019.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. The rise of big data: how it's changing the way we think about the world. *Foreign Affairs*, New York, v. 92, n. 3, May-June 2013. Disponível em: http://tiny.cc/9o5ycz. Acesso em: 18 set. 2019.

D'ANGELO, André Cauduro. A ética no marketing. *Revista de Administração Contemporânea*, Maringá, PR, v. 7, n. 4, p. 55-75. dez. 2003. Disponível em: http://dx.doi.org/10.1590/S1415-65552003000400004. Acesso em: 25 set. 2019.

DAVIES, Nigel; LANGHEINRICH, Marc. Privacy by design [from the Editor in Chief]. *IEEE Pervasive Computing*, Lugano, Switzerland, v. 12, n. 2, p. 2-4, Apr. 2013. Disponível em: https://ieeexplore.ieee.org/document/6504852. Acesso em: 25 jun. 2019.

DONEDA, Danilo; ALMEIDA, Virgilio A. F. What is algorithm governance? *IEEE Internet Computing*, Nicosia, Cyprus, v. 20, n. 4, p.60-63, Jul. 2016. Disponível em: https://ieeexplore.ieee.org/document/7529042. Acesso em: 18 nov. 2019.

DRAPER, Roger. The Faithless Shepherd. *The New York Review of Books*, New York, 26 jun. 1986. Disponível em: https://www.nybooks.com/articles/1986/06/26/the-faithless-shepherd/. Acesso em: 4 nov. 2019.

ECKERSLEY, Peter. How unique is your web browser? *In*: ATALLAH, Mikhail J.; HOPPER, Nicholas J. (org.). INTERNATIONAL CONFERENCE ON PRIVACY ENHANCING TECHNOLOGIES: PETS'10, 10., 2010, Berlin. *Proceedings* [...]. Berlin: Springer-Verlag, 2010. Disponível em: https://panopticlick.eff.org/static/browser-uniqueness.pdf. Acesso em: 30 set. 2019.

ENGLEHARDT, Steven; NARAYANAN, Arvind. Online tracking: a 1-million-

-site measurement and analysis. *In*: CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY: ACM SIGSAC, 2016, Vienna. *Proceedings* [...]. Vienna, Áustria: ACM SIGSAC, 2016. Disponível em: http://bit.do/fa-6PJ. Acesso em: 29 de nov. de 2018.

ENGLICH, Birte; MUSSWEILER, Thomas; STRACK, Fritz. Playing dice with criminal sentences: the influence of irrelevant anchors on experts' judicial decision making. *Personality and Social Psychology Bulletin*, [Los Angeles, CA], v. 32, n. 2, p. 188-200, Febr. 2006. Disponível em: https://www.ncbi.nlm.nih.gov/pubmed/16382081. Acesso em: 5 out. 2019.

FERNANDES, André Dias. Terrorismo, Lei do Abate e direito à segurança na sociedade de risco. *Revista Nomos*, Fortaleza, v. 35, n. 2, p. 43-65, 2015. Disponível em: http://periodicos.ufc.br/nomos/article/view/1435. Acesso em: 21 jun. 2019.

FOLJANTY, Lena. Legal transfers as processes of cultural translation: on the consequences of a metaphor. *Max Planck Institute for European Legal History Research Paper Series*, [Berlin], n. 2015-09, 2015. Disponível em: https://ssrn.com/abstract=2682465. Acesso em: 12 nov. 2019.

GERSTEIN, Robert S. Intimacy and privacy. *Ethics*, Chicago, v. 89, n. 1, p. 76-81, 1978. Disponível em: www.jstor.org/stable/2380133. Acesso em: 18 mar. 2019.

GILPIN, Leilani H. *et al.* Explaining explanations: an overview of interpretability of machine learning. *In:* IEEE INTERNATIONAL CONFERENCE ON DATA SCIENCE AND ADVANCED ANALYTICS: DSAA, 5., 2018, Turin, IT. *Proceedings* [...]. Turin, IT: Data Science and Advanced Analytics, DSSA, out. 2018. p. 1-10. Disponível em: https://arxiv.org/abs/1806.00069#. Acesso em: 27 set. 2019.

GINSBERG, Jeremy; MOHEBBI, Matthew; PATEL, Rajan. *et al.* Detecting influenza epidemics using search engine query data. *Nature,* London, v. 457, n. 7232, p. 1012–1014, 2009. Disponível em: https://www-nature.ez11.periodicos.capes.gov.br/articles/nature07634. Acesso em: 18 set. 2019.

HARTUNG, Pedro Afonso Duarte; KARAGEORGIADIS, Ekaterine Valente. A regulação da publicidade de alimentos e bebidas não alcoólicas para

crianças no Brasil. *Revista de Direito Sanitário*, São Paulo, v. 17, n. 3, p. 160-184, mar. 2017. Disponível em: <http://www.revistas.usp.br/rdisan/article/view/127783. Acesso em: 14 jun. 2019.

HELLES, Rasmus; FLYVERBOM, Mikkel. Meshes of surveillance, prediction, and infrastructure: on the cultural and commercial consequences of digital platforms. *Surveillance & Society*, Chapel Hill, NC, v. 17, n. 1/2, p.34-39, mar. 2019. Disponível em: http://dx.doi.org/10.24908/ss.v17i1/2.13120. Acesso em: 24 set. 2019.

HIRSCH, Dennis. predictive analytics law and policy: a new field emerges. *I/S*: A Journal of Law and Policy For The Information Society, Ohio, v. 14, n. 1, p. 1-9, 2017. Disponível em: http://hdl.handle.net/1811/86703. Acesso em: 24 set. 2019.

HOOFNAGLE, Chris Jay, SOLTANI, Ashkan *et al.* Behavioral advertising: the offer you cannot refuse. *Harvard Law & Policy Review,* Cambridge, MA, v. 6, p. 273-293, 2012. Disponível em: https://ssrn.com/abstract=2137601. Acesso em: 4 out. 2019.

HU, Margaret. Big Data Blacklisting. *Florida Law Review*, Florida, v. 67, n. 5, p.1735-1809, 2016. Disponível em: https://scholarship.law.ufl.edu/flr/vol67/iss5/5. Acesso em: 24 set. 2019.

KAHN, Peter H. *et al.* "Robovie, you'll have to go into the closet now": children's social and moral relationships with a humanoid robot. *Developmental Psychology*, Washington, DC, v. 48, n. 2, p. 303-314, mar. 2012. Disponível em: https://psycnet.apa.org/fulltext/2012-04837-001.html. Acesso em: 4 out. 2019.

KHAN, Lina M. Amazon's Antitrust Paradox. *Yale Law Journal*, New Haven, v. 126, n. 3, p. 710-805, 2016. Disponível em: https://digitalcommons.law.yale.edu/ylj/vol126/iss3/3/. Acesso em: 9 ago. 2019.

KOMENO, Eliana Matiko *et al.* Velocidade de leitura e desempenho escolar na última série do ensino fundamental. *Estudos de Psicologia,* Campinas, v. 32, n. 3, p. 437-447. set. 2015. Disponível em: http://www.scielo.br/pdf/estpsi/v32n3/0103-166X-estpsi-32-03-00437.pdf. Acesso em: 26 mar. 2019.

KOOPS, Bert-jaap; HOEPMAN, Jaap-henk; LEENES, Ronald. Open-source

intelligence and privacy by design. *Computer Law & Security Review*, [Amsterdan], v. 29, n. 6, p. 676-688, dez. 2013. Disponível em: http://dx.doi.org/10.1016/j.clsr.2013.09.005. Acesso em: 24 jun. 2019.

LANEY, Doug. 3D data management: controlling data volume, velocity, and variety. *Application Delivery Strategies*, fev. 200, p. 1-4, 2012. Disponível em: https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso em: 18 set. 2019.

LEMLEY, Mark A. Terms of use. *Minnesota Law Review,* Minneapolis, MN, v. 91, p. 459-483, 2006. Disponível em: https://ssrn.com/abstract=917926. Acesso em: 24 jun. 2019.

LEON, Pedro *et al.* Why Johnny can't opt out. *In:* SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS: CHI '12, 12., New York, 2012. *Proceedings* [...]. New York: ACM Press, 2012. p. 1-10. Disponível em: http://dx.doi.org/10.1145/2207676.2207759. Acesso em: 29 set. 2019.

LERMAN, Jonas. Big data and its exclusions. *Stanford Law Review Online*, Stanford, v. 66, p. 55-63, Sept. 2013. Disponível em: http://dx.doi.org/10.2139/ssrn.2293765. Acesso em: 20 set. 2019.

LOVISON, Aida Maria; PETROLL, Martin de La Martinière. Ética na publicidade e propaganda: a visão do executivo de agências de comunicação do Rio Grande do Sul. *Cadernos Ebape.br*, São Paulo, v. 9, n. 2, p. 333-359. jun. 2011. Disponível em: http://dx.doi.org/10.1590/S1679-39512011000200007. Acesso em: 25 set. 2019.

MAGRANI, Eduardo. New perspectives on ethics and the laws of artificial intelligence. *Internet Policy Review,* Berlin, v. 8, n. 3, 2019. Disponível em: https://policyreview.info/articles/ analysis/new-perspectives-ethics-and--laws-artificial-intelligence. Acesso em: 18 nov. 2019.

MASKE, Carel. Competition policy and the digital single market in the wake of brexit: is geoblocking always as evil as most consumers believe? *Journal of European Competition Law & Practice*, Oxônia, v. 7, n. 8, p. 509-510, ago. 2016. Disponível em: http://dx.doi.org/10.1093/jeclap/lpw069. Acesso em: 2 out. 2019.

MCDONALD, A. M., CRANOR, L. F. The cost of reading privacy policies. *I/S*: A Journal of Law and Policy for the Information Society, Ohio, v. 4, n. 3, p. 543-568, 2008. Disponível em: http://hdl.handle.net/1811/72839. Acesso em: 20 jun. 2019.

MCNULTY, Eileen. Understanding big data: the seven v's. *Dataconomy,* Berlin, 22nd. May 2014. Disponível em: http://dataconomy.com/2014/05/seven-vs-big-data/. Acesso em: 18 set. 2019.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? *Instituto Igarapé*: a think and do tank, Rio de Janeiro, n. 39, p. 1-17, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 18 nov. 2019.

MONTJOYE, Y.-a. de *et al*. Unique in the shopping mall: on the reidentifiability of credit card metadata. *Science*, Washington, DC., v. 347, n. 6221, p. 536-539, 29 jan. 2015. Disponível em: https://science.sciencemag.org / content/347/6221/536/tab-pdf. Acesso em: 15 nov. 2019.

PATGIRI, Ripon, AHMED, Arif. Big Data: The V's of the Game Changer Paradigm. *In*: IEEE HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS, 18., 2016, Sydney. *Proceedings* [...]. Sydney: IEEE, 2016. Disponível em: http://tiny.cc/honbdz. Acesso em: 24 set. 2019.

PICKER, Randal C. Online advertising, identity and privacy. John M. Olin Law & Economics Working Paper, Chicago, n. 475, p. 1-44, jul. 2009. Disponível em: http://dx.doi.org/10.2139/ssrn.1428065. Acesso em: 28 set. 2019.

RIJMENAM, Mark van. Why the 3 v's are not sufficient to describe big data. *Datafloq,* Hague, ago. 2015. Disponível em: https://datafloq.com/read/3vs-sufficient-describe-big-data/166. Acesso em: 18 set. 2019.

ROCHET, Jean-Charles; TIROLE, Jean. Defining Two Sided Markets. *IDEI*, Toulouse, p. 1-28, 2004. Disponível em: http://tiny.cc/z52ycz. Acesso em: 18 set. 2019.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. *Direito, Estado e Sociedade,* Rio de Janeiro, v. 36, n. 1, p.178-199, jun. 2010. Disponível

em: http://direitoestadosociedade.jur.puc-rio.br/cgi/cgilua.exe/sys/start.htm?infoid=180&sid=18. Acesso em: 14 mar. 19.

SIMON, Herbert A. A behavioral model of rational choice. *The Quarterly Journal Of Economics*, Cambridge, MS, v. 69, n. 1, p. 99-118, fev. 1955. Disponível em: https://www.jstor.org/stable/1884852. Acesso em: 14 jun. 2019.

SOLTANI, Ashkan *et al.* Flash cookies and privacy. *SSRN Electronic Journal*, [S.l.], p. 1-8, 2009. Disponível em: http://dx.doi.org/10.2139/ssrn.1446862. Acesso em: 30 set. 2019.

STEINFELD, Nili. "I agree to the terms and conditions": (how) do users read privacy policies online?: an eye-tracking experiment. *Computers In Human Behavior*, Amsterdam, v. 55, p. 992-1000, Fev. 2016. Disponível em: http://tiny.cc/r79raz. Acesso em: 5 ago. 2019.

SUNSTEIN, Cass R.; THALER, Richard. A behavioral approach to law and economics. *Stanford Law Review*, Stanford, v. 50, n. 5, p. 1471-1550, May 1998. Disponível em: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=12172&context=journal_articles. Acesso em: 14 jun. 2019.

TENE, Omer; POLONETSKY, Jules. A theory of creepy: technology, privacy, and shifting social norms. *Yale Journal of Law & Technology*, New Haven, v. 16, n. 1, p. 59-102, 2014. Disponível em: https://digitalcommons.law.yale.edu/yjolt/vol16/iss1/2/. Acesso em: 29 set. 2019.

VEIL, Winfried. The GDPR: the emperor's new clothes: on the structural shortcomings of both the old and the new Data Protection Law. *Neue Zeitschrift für Verwaltungsrech,* München, v. 10, p. 686-696, 2018. Disponível em: https://ssrn.com/abstract=3305056. Acesso em: 12 nov. 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Boston, v. 4, n. 5, p. 193-220, 15 Dec. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 13 fev. 2019.

WACHTER, Sandra, MITTELSTADT Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review,* New York, n. 2, p. 1-130, 2019. Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 27 set. 2019.

WANG, Yang *et al.* Privacy nudges for social media: na exploratory Facebook study. *In:* INTERNATIONAL CONFERENCE ON WORLD WIDE WEB: WWW '13 COMPANION, 22., 2013, Rio de Janeiro, RJ. *Proceedings* [...]. New York: ACM Press, 2013. p. 1-8. Disponível em: http://precog.iiitd.edu.in/events/psosm2013/9psosm6-wang.pdf. Acesso em: 5 out. 2019.

WEISER, Mark. The computer for the 21st Century. *SIGMOBILE Mobile Review,* [S.l.], n. 3, p. 3-11, July 1999. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf. Acesso em: 25 de nov. de 2018.

WEST, Emily. Amazon: Surveillance as a service. *Surveillance & Society*, Chapel Hill, NC, v. 17, n. 1/2, p. 27-33. 31 Mar. 2019. Disponível em: https://doi.org/10.24908/ss.v17i1/2.13008. Acesso em: 4 out. 2019.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. *Revista Brasileira de Direito Civil*, Belo Horizonte, v. 3, n. 1, p. 8-27, mar. 2015. Disponível em: https://www.ibdcivil.org.br/image/data/revista/volume3/02---rbdcivil-volume-3---o-surgimento-e-o-desenvolvimento-do-right-of-privacy-nos-estados-unidos.pdf. Acesso em: 12 mar. 2019.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, London, v. 30, n. 1, p. 75-89, Mar. 2015. Disponível em: http://dx.doi.org/10.1057/jit.2015.5. Acesso em: 14 mar. 2019.

Teses e Dissertações

VIEIRA, Karla Patrícia de Castro Almeida. *A proteção jurídica do direito à privacidade e a incolumidade dos dados pessoais em face do avanço da informática.* 2001. Dissertação (Mestrado em Direito) – Pós-Graduação em Direito, Universidade Federal do Ceará, Fortaleza, 2001.

Documentos Jurídicos e Relatórios Científicos

ESPANHA. Agência Espanhola de Proteção de Dados. *Resolución: R/01870/2017*. Madrid: AEPD, 11 set. 2017. Disponível em: https://www.

aepd.es/resoluciones/PS-00082-2017_REC.pdf. Acesso em: 5 out. 2019.

ALEMANHA. Bundeskartellamt. *Administrative Proceedings Decision under Section, v. 32, n. 1, German Competition Act (GWB) B6-22/16.* Bonn, 6 fev. 2019. Disponível em: http://tiny.cc/xnu3cz. Acesso em: 20 set. 2019.

ALEMANHA. *Lei Fundamental da República Federal da Alemanha*. Disponível em: https://www.btg-bestellservice.de/pdf/80208000.pdf. Acesso em: 19 mar. 2019.

BRASIL. Banco Central do Brasil. *Circular n. 3.461 de 24/7/2009*. Brasília, DF: Banco Central do Brasil, 2009. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3461. Acesso em: 26 nov. 2019.

BRASIL. Câmara dos Deputados. Ato da Presidência de 15/10/2019. *Diário Oficial da Câmara dos Deputados*, Brasília, DF, ano 74, supl., n. 186, 16 out 2019. Disponível em: http://tiny.cc/xqhsgz. Acesso em: 24 nov. 2019.

BRASIL. Congresso Nacional. *Veto n. 24/2019 (Proteção de dados pessoais).* Brasília, DF: Congresso Nacional, 2019. Disponível em: http://tiny.cc/bbeugz. Acesso em: 25 nov. 2019.

BRASIL. Congresso Nacional. *Veto n. 24/2019.* Votação do dispositivo 24.19.001 – § 3º do art. 20 da Lei n. 13.709, de 14 de Agosto de 2018, com a redação dada pelo art. 2º do projeto. Brasília, DF: Congresso Nacional, 2019. Disponível em: https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445/1. Acesso em: 17 nov. 2019.

BRASIL. Departamento de Defesa e Proteção do Consumidor. *A proteção de dados pessoais nas relações de consumo*: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. Disponível em: https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 6 nov. 2019

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Estratégia brasileira para a transformação digital*: e-digital. Brasília, DF: Ministério da Ciência, Tecnologia, Inovações e Comunicações, 2018. Disponível em: http://www.mctic.gov.br/mctic/export/sites/institucional/estrategiadigital.pdf. Acesso em: 6 nov. 2019.

BRASIL. Ministério da Justiça. *Debate público proteção de dados pessoais.* Brasília, DF: Ministério da Justiça, 2011. Disponível em: http://pensando.mj.gov.br/dadospessoais2011/debata-a-norma/. Acesso em: 6 nov. 2019.

BRASIL. Ministério da Justiça. *Despacho n. 299/2018.* Brasília, DF: Ministério da Justiça, 2018. Disponível em: http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/26176368/do1-2018-06-18-despacho-n-299-2018-26176301. Acesso em: 3 de out. de 2019.

BRASIL. Ministério da Justiça. *Nota Técnica n. 92/2018/CSA-SENACON/CGCTSA/GAB-DPDC/DPDC/SENACON/MJ.* Brasília, DF: Ministério da Justiça, 2018. Disponível em: http://tiny.cc/x4hwdz. Acesso em: 3 de out. de 2019.

BRASIL. Ministério do Planejamento, Desenvolvimento e Gestão. *Estratégia de Governança Digital:* Transformação Digital: cidadania e governo. Brasília, DF: Ministério do Planejamento, 2018. Disponível em: https://www.governodigital.gov.br/EGD/documentos/revisao-da-estrategia-de-governanca-digital-2016-2019.pdf. Acesso em: 25 nov. 2019.

BRASIL. Presidência da República. *Mensagem n. 451, de 14 de agosto de 2018*. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 6 nov. 2019.

BRASIL. Presidência da República. *Mensagem n. 288/2019*. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 17 nov. 2019.

BRASIL. Senado Federal. *Projeto de Lei n. 330/2013.* Brasília, DF: Senado Federal, 2013. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1567533189697&disposition=inline. Acesso em: 1º dez. 2019.

BRASIL. Senado Federal. *Proposta de Emenda à Constituição n. 17 de 2019.* Brasília, DF: Senado Federal, 2019. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7924709&ts=1571776978885&disposition=inline. Acesso em: 11 nov. 2019.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial n. 1.419.697/RS*

(2013/0386285-0). Relator: Paulo de Tarso Sanseverino, 12 de novembro de 2014. Brasília, DF: Superior Tribunal de Justiça, 17 nov. 2014. Disponível em: http://tiny.cc/kvhdgz. Acesso em: 16 nov. 2019.

BRASIL. Superior Tribunal de Justiça. *Súmula 403.* Brasília, DF, 28 de outubro de 2009. Brasília, DF: Superior Tribunal de Justiça, 24 nov. 2009. Disponível em: https://scon.stj.jus.br/SCON/sumstj/toc.jsp?livre=sumula.tipo.%20e%20%20403.num. Acesso em: 18 nov. 2019.

BRASIL. Superior Tribunal de Justiça. *Súmula 550*. Brasília, DF, 14 de outubro de 2015. Brasília, DF: Superior Tribunal de Justiça, 19 out. 2015. Disponível em: https://scon.stj.jus.br/SCON/sumanot/toc.jsp?livre=(sumula%20adj1%20%20550).sub. Acesso em: 18 nov. 2019.

BRASIL. Supremo Tribunal Federal. *ADI 4815 DF.* Relatora: Min. Cármen Lúcia, 1 fev. 2016. Disponível em: http://www.stf.jus.br/portal/peticaoInicial/verPeticaoInicial.asp?base=ADI&documento=&s1=4815&numProcesso=4815. Acesso em: 18 mar. 2019.

CHECKMARX. *Amazon echo:* Alexa Leveraged as a silent eavesdropper. Ramat Gan: Checkmarx, 2018. Disponível em: https://info.checkmarx.com/hubfs/Amazon_Echo_Research.pdf. Acesso em: 5 out. 2019.

COMISSÃO EUROPEIA. *Binding Corporate Rules (BCR):* corporate rules for data transfers within multinational companies. Bruxelas, 2019. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en. Acesso em: 15 nov. 2019.

COMISSÃO EUROPEIA. *Case M.8228:* Facebook/Whatsapp. 17.05.2017. Disponível em: https://ec.europa.eu/competition/mergers/cases/decisions/m8228_493_3.pdf. Acesso em: 20 set. 2019.

COMISSÃO EUROPEIA. *Decisão 2004/915/EC:* Standard Contractual Clauses (SCC). EUR-Lex, Luxembourg, 2019. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915. Acesso em: 15 nov. 2019.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (França). *Délibération n. SAN-2019-001 du 21 janvier 2019:* délibération de la formation restreinte n. SAN – 2019-001 du 21 janvier 2019 pro-

nonçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC. 2019. Disponível em: https://www.legifrance.gouv.fr/affichCnil.do?&id=CNILTEXT000038032552. Acesso em: 14 jun. 2019.

CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) 2018/302.* EUR-Lex, Luxembourg, 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R0302&fro m=EN. Acesso em: 2 out. 2019.

ESPANHA. [Constituição (1978)]. *Constitución Española= Constituição Espanhola.* [Madrid]: Junta de Castilla y León, [1992]. 46 p. Disponível em: https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf. Acesso em: 3 jun. 2019.

ESTADOS UNIDOS. *Online Privacy Act*. Washington, D.C., 2019. Disponível em: http://tiny.cc/rvz7fz. Acesso em: 13 nov. 2019.

ESTADOS UNIDOS. *Patent n. 45*. Date of Patent: US 9,928,406 B2, 27 Mar. 2018. Disponível em: https://patentimages.storage.googleapis.com/69/7c/bd/e24c7a6c86972d/US9928406.pdf. Acesso em: 3 out. 2019.

GOMEZ, Joshua; PINNICK, Travis; SOLTANI, Ashkan. *Know privacy*. UC Berkeley, School of Information, Berkeley, CA, 2009. Disponível em: http://knowprivacy.org/full_report.html. Acesso em: 29 set. 2019.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Projeção da população do Brasil e das Unidades da Federação.* Rio de Janeiro: IBGE, [2019]. Disponível em: https://www.ibge.gov.br/apps/populacao/projecao/. Acesso em: 17 jun. 2019.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. *Tabela 5919*: população por níveis de instrução. Rio de Janeiro: IBGE, [2021]. Disponível em: https://sidra.ibge.gov.br/tabela/5919#resultado. Acesso em: 17 jun. 2019.

INSTITUTO DE TECNOLOGIA E SOCIEDADE. *Lei Geral de Proteção de Dados Pessoais (LGPD) e Setor público*: um guia da lei 13.709/2018, voltado para os órgãos e entidades públicas. Rio de Janeiro: ITS, 2019. p. 13. Disponível em: http://tiny.cc/uaqugz. Acesso em: 25 nov. 2019.

NAÇÕES UNIDAS. *Declaração Universal dos Direitos Humanos.* [New York]: United Nations, 2018. Disponível em: https://nacoesunidas.org/wp-con-

tent/uploads/2018/10/DUDH.pdf. Acesso em: 19 mar. 2019.

NAÇÕES UNIDAS. General Assembly. *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.* [New York]: United Nations, 16 May 2011. 22. p. (Human Rights Council; 17/27). Disponível em: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Acesso em: 15 jun. 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Big data*: bringing competition policy to the digital era. Paris: OECD, 2016. 40 p. (DAF/COMP; n. 14). Disponível em: http://tiny.cc/yg4ycz. Acesso em: 18 set. 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Digital Government Review of Brazil*: towards the digital transformation of the public sector. Paris: OECD Publishing, 28 nov. 2018. 146 p. (OECD Digital Government Studies). Disponível em: http://www.oecd.org/governance/digital-government-review-of-brazil-9789264307636-en.htm. Acesso em: 6 nov. 2019.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. *Exploring the economics of personal data:* a survey of methodologies for measuring monetary value. Paris: OECD Publishing, 2 abr. 2013. 39 p. (OECD Digital Economy Papers; n. 220). Disponível em: http://dx.doi.org/10.1787/5k486qtxldmq-en. Acesso em: 30 set. 2019.

PANOPTYKON FOUNDATION. *Profiling the unemployed in Poland:* social and political implications of algorithmic decision making. Warsaw: Panoptykon Foundation, 2015. 51 p. Disponível em: https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf. Acesso em: 27 set. 2019.

PARLAMENTO EUROPEU. European Parliamentary Research Service. *From safe harbour to privacy shield: advances and shortcomings of the new EU-US data transfer rules.* European Parliament, London, 2017. Disponível em: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf. Acesso em: 14 nov. 2019.

PARLAMENTO EUROPEU. Conselho da União Europeia. *Directiva 95/46/CE*

do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. EUR-Lex, Luxembourg, [2003]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 15 jun. 2019.

PARLAMENTO EUROPEU. Conselho da União Europeia. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.* EUR-Lex, Luxembourg, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX:32016R0679. Acesso em: 15 jun. 2019.

PORTUGAL. [Constituição (1976)]. *Constituição da República Portuguesa.* [Lisboa]: Assembleia Constituinte, 1976. Disponível em: https://www.parlamento.pt/Legislacao/paginas/constituicaorepublicaportuguesa.aspx. Acesso em: 3 jun. 2019.

REINO UNIDO. Information Commissioner's Office. *Big Data, artificial intelligence, machine learning and data protection.* London: ICO, 2017. Disponível em: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf. Acesso em: 18 nov. 2019.

REINO UNIDO. Information Commissioner's Office. *Lawful basis for processing.* London: ICO, 2019. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Acesso em: 29 nov. 2019.

REINO UNIDO. Information Commissioner's Office. What is the balancing test? London: ICO, 2019. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Acesso em: 27 nov. 2019.

UNIÃO EUROPEIA. Court of Justice. *Judgment in case C-40/17.* Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. Luxembourg: Court of Justice of the European Union, 2019. Disponível em: https://curia.europa.

eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf. Acesso em: 12 nov. 2019.

UNIÃO EUROPEIA. Court of Justice (Grand Chamber). *Judgment of the Court Case C-362/14.* Maximillian Schrems v Data Protection Commissioner, joined party: digital rights Ireland Ltd. Luxembourg: Court of Justice of the European Union, 2015. Disponível em: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195 &pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=125031. Acesso em: 12 nov. 2019.

UNESCO. *I'd blush if I could:* closing gender divides in digital skills through education. Paris: Organização das Nações Unidas para a Educação, 2019. 145 p. Disponível em: http://tiny.cc/uslydz. Acesso em: 4 out. 2019.

WISCONSIN. Supreme Court. *State v. Loomis.* 881 N.W.2d 749. Wi 68 2016. Madison: Supreme Court, 2016. Disponível em: http://tiny.cc/xjvidz. Acesso em: 27 set. 2019.

Palestras e Congressos

HIRSCH, Dennis. *Keynote* 2: além do controle: reinventando a lei de privacidade para a economia algorítmica. *In*: SEMINÁRIO DE PROTEÇÃO À PRIVACIDADE AOS DADOS PESSOAIS, 10., 2019, São Paulo. *Anais* [...]. São Paulo: NIC.br; CGI.br, 2019. 1 vídeo (210 min.). Disponível em: https://www.youtube.com/watch?v=YMoXqvNhFSw&t=5852s. Acesso em: 1 out. 2019.

LEONARDI, Marcel. A empresa e a proteção de dados (Lei N. 13.709/18). *In*: CONGRESSO BRASILEIRO DE DIREITO COMERCIAL, 9., 2019, São Paulo. *Anais* [...]. São Paulo: ACDCOM, 2019. Disponível em: https://www.congressodireitocomercial.org.br/site/congressos/9-congresso-brasileiro-de-direito-comercial. Acesso em: 17 jun. 19.

SATTERFIELD, Stephen. Algoritmos, inteligência artificial e proteção de dados. *In*: SEMINÁRIO DE PROTEÇÃO À PRIVACIDADE AOS DADOS PESSOAIS, 10., São Paulo, 2019. *Anais* [...]. São Paulo: NIC.br; CGI.br, 2019. 1 vídeo (210 min.). Disponível em: https://www.youtube.com/watch?v=hZNGOT0JN_M&t=12491s. Acesso em: 1 out. 2019.

SOUSA, Marcos Andrey de. As investigações internas e a Proteção de

Dados (Lei n. 13.709/18). *In*: CONGRESSO BRASILEIRO DE DIREITO COMERCIAL, 9., São Paulo, 2019. *Anais* [...]. São Paulo: ACDCOM, 2019. Disponível em: https://www.congressodireitocomercial.org.br/site/arquivo-de-videos/videos-do-9o-congresso/#video-gallery-b744ef9-22, 05:30 – 06:13 minutos. Acesso em: 17 jun. 19.

UNIÃO EUROPEIA. Comissão Europeia. *Ethics guidelines for trustworthy AI=Orientações éticas para uma IA de confiança.* Brussels: European Commission, GPAN IA, 2018. Disponível em: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. Acesso em: 18 nov. 2019.

Prefácios, apresentações e introduções de obras

PEPPERS, Don; ROGERS, Martha. Prefácio. *In*: KASANOFF, Bruce. *Atendimento personalizado e o limite da privacidade*: até que ponto as empresas podem usar informações pessoais para lucrar na internet. Rio de Janeiro: Campus, 2002.

Outros textos em meios eletrônicos

ABREU, Jacqueline; LAGO, Lucas; MASSARO, Heloisa. Por que se preocupar com o que o Estado faz com nossos dados pessoais? *Internetlab,* São Paulo, maio 2018. Disponível em: http://www.internetlab.org.br/pt/privacidade-e-vigilancia/especial-apps-do-governo/. Acesso em: 24 nov. 2019.

AMIGO, Ignacio. The metro stations of São Paulo that read your face. *CityLab,* New York, Disponível em: https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/. Acesso em: 3 out. 2019.

AMOROS, Raul. A century of America's top 10 companies, in one chart. *Howmuch.net*, [S.l.], 2017. Disponível em: http://tiny.cc/ojdf8y. Acesso em: 17 jun. 2019.

ANDROID Flashlight App Developer Settles FTC Charges It Deceived Consumers. *FTC website,* [S.l.], 2013. Disponível em: https://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-set-

tles-ftc-charges-it-deceived. Acesso em: 15 mar. 2019.

AUTONOMOUS System Number (ASN). *Techopedia*, Edmonton, AB, [2019]. Disponível em: https://www.techopedia.com/definition/26871/autonomous-system-number-asn. Acesso em: 30 set. 2019.

AV-TEST. *AV-TEST Awards 2018 go to Kaspersky Lab.* [S.l.], 2019. Disponível em: https://www.av-test.org/en/news/av-test-awards-2018-go-to-kaspersky-lab/. Acesso em: 1 out. 2019.

BADSHAH, Nadeem. Facebook to contact 87 million users affected by data breach. *The Guardian.* London, 2018. Disponível em: https://www.theguardian.com/technology/2018/apr/08/ facebook-to-contact-the-87-million-users-affected-by-data-breach. Acesso em: 25 abr. 2019.

BARR, Sabrina. Amazon's Alexa to reward children who behave politely. *Independent,* London, 2018. Disponível em: https://www.independent.co.uk/life-style/health-and-families/amazon-alexa-reward-polite-children-manners-voice-commands-ai-america-a8325721.html. Acesso em: 4 out. 2019.

BIONI, Bruno R. De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados. *Jota*, São Paulo, 2018. Disponível em: www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em: 6 nov. 2019.

BOGOST, Ian. My cow game extracted your Facebook data. *The Atlantic, Boston*, Massachusetts, 2018. Disponível em: https://www.theatlantic.com/technology/archive/2018/03/my-cow-game-extracted-your-facebook-data/556214/. Acesso em: 19 jun. 2019.

BOHN, Dieter. Amazon says 100 million Alexa devices have been sold – what's next? *The Verge,* New York, 2019. Disponível em: https://www.theverge.com/2019/1/4/18168565/amazon-alexa-devices-how-many-sold-number-100-million-dave-limp. Acesso em: 4 out. 2019

BRASIL. Ministério da Economia. *O que é o TaxiGov.* Brasíia, DF: Ministério da Economia, [2019]. Disponível em: http://www.economia.gov.br/assuntos/gestao/taxigov. Acesso em: 28 nov. 2019.

BRASIL. Ministério da Justiça e Segurança Pública. *Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet.* Brasília, DF: Ministério da Justiça, 23 jul. 2019. Disponível em: https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em: 6 nov. 2019.

CHAVEZ, Nicole. Arkansas judge drops murder charge in Amazon Echo case. *CNN,* New York, 2017. Disponível em: https://edition.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html. Acesso em: 5 out. 2019.

CHOKSHI, Niraj. Is Alexa listening? Amazon Echo sent out recording of couple's conversation. *The New York Times*, New York, 2018. Disponível em: https://www.nytimes.com /2018/05/25/business/amazon-alexa-conversation-shared-echo.html. Acesso em: 5 out. 2019.

COELHO, Jorge. Turismo online no Brasil fatura R$ 35,1 bilhões. *Fecomércio*, Aracaju, 2018. Disponível em: http://www.fecomercio-se.com.br/radarfecomercio/radar-120. Acesso em: 3 out. 2019.

COOK, James. Amazon patents new Alexa feature that knows when you're ill and offers you medicine. *Telegraph*, London, 2018. Disponível em: https://www.telegraph.co.uk/technology/2018/10/09/amazon-patents-new-alexa-feature-knows-offers-medicine/. Acesso em: 4 out. 2019.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*, London, 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 24 set. 2019.

DAY, Matt *et al.* Amazon workers are listening to what you tell Alexa. *Bloomberg,* New York, 2019. Disponível em: https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio. Acesso em: 5 out. 2019.

DE LUCA, Cristina. Decreto de Bolsonaro aproxima uso de nossos dados a países como China. Blog Porta 23. *UOL,* Rio de janeiro, out. 2019. Disponível em: https://porta23.blogosfera.uol.com.br/2019/10/13/governo-

-tem-nossos-dados-mas-nao-deve-trata-los-como-se-fosse-o-dono-deles. Acesso em: 24 nov. 2019.

DELGADO, Márcia. Serpro é suspeito de vender dados pessoais para administração pública. *Metrópoles,* Brasília, DF, maio 2018. Disponível em: https://www.metropoles.com/distrito-federal/serpro-e-suspeito-de-vender-dados-pessoais-para-administracao-publica. Acesso em: 24 nov. 2019.

DOSHI, Vidhi. A security breach in India has left a billion people at risk of identity theft. *Washington Post,* Washington, D.C., 2018. Disponível em: https://www.washingtonpost.com/news/worldvie ws/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?noredirect=on. Acesso em: 15 mar. 2019.

DUHIGG, Charles. How companies learn your secrets. *The New York Times Magazine*, New York, 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp. Acesso em: 1º out. 2019.

EUROPEAN DATA PROTECTION SUPERVISOR. *The history of the general data protection regulation.* [London]: EDPS, 2018. Disponível em: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 12 nov. 2019.

FACEBOOK finaliza aquisição do Whatsapp por US$ 22 bilhões. *Portal G1*, [Rio de Janeiro], 2014. Disponível em: http://tiny.cc/liui8y. Acesso em: 19 jun. 2019.

FESSLER, Leah. We tested bots like Siri and Alexa to see who would stand up to sexual harassment. *Quartz*, New York, 2017. Disponível em: https://qz.com/911681/we-tested-apples-siri-amazon-echos-alexa-microsofts-cortana-and-googles-google-home-to-see-which-personal-assistant-bots-stand-up-for-themselves-in-the-face-of-sexual-harassment/. Acesso em: 4 out. 2019.

GAVIOLI, Alan. Falha no sistema do Detran-RN causa vazamento de dados de 70 milhões de brasileiros. *Infomoney*, São Paulo, 2019. Disponível em: https://www.infomoney.com.br/minhas-financas/falha-no-sistema-do-detran-rn-causa-vazamento-de-dados-de-70-milhoes-de-brasileiros/. Acesso em: 29 nov. 2019.

HODGSON, Sam. Edward Snowden: 'do i think things are fixed? no.' *The New York Times*, New York, 2016. Disponível em: https://www.nytimes.com/2016/12/07/opinion/edward-snowden-do-i-think-things-are-fixed-no.html. Acesso em: 4 jun. 2019.

HOHMAN, Maura. Man divorces wife after accidentally catching her cheating on google maps street view. *People*, New York, 2018. Disponível em: https://people.com/home/man-catches-wife-cheating-google-maps-street-view-they-divorce/. Acesso em: 5 jan. 2020.

INSTAGRAM. *Central de privacidade e segurança.* [Menlo Park, CA], 2019. Disponível em: http://tiny.cc/o8387y. Acesso em: 13 jun. 2019.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. *Approved binding corporate rules.* Portsmouth, NH: IAPP, 2020. Disponível em: https://iapp.org/resources/article/approved-binding-corporate-rules/. Acesso em: 17 nov. 2019.

INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS. *Infographic*: GDPR: one year anniversary. Portsmouth, NH: IAPP, [2018]. Disponível em: http://tiny.cc/ae27fz. Acesso em: 12 nov. 2019.

JEONG, Sarah. Zuckerberg struggles to name a single Facebook competitor. *The Verge,* New York, 10 abr. 2018. Disponível em: https://www.theverge.com/2018 /4/10/17220934/facebook-monopoly-competitor-mark-zuckerberg-senate-hearing-lindsey-graham. Acesso em: 19 set. 2019.

LAMANCE, Ken. Shrink wrap agreement lawyers. *Legal Match*, San Francisco, CA, [2018]. Disponível em: https://www.legalmatch.com/law-library/article/shrink-wrap-agreements.html. Acesso em: 25 jun. 2019.

LEMOS, Ronaldo. Proposta de Doria de vender os dados do bilhete único é ilegal. *Folha de São Paulo,* São Paulo, fevereiro 2017. Disponível em: https://www1.folha.uol.com.br/ colunas/ronaldolemos/2017/02/1860214-proposta-de-doria-de-vender-os-dados-do-bilhete-unico-e-ilegal.shtml. Acesso em: 24 nov. 2019.

LEORATTI, Alexandre. Leis de dados pessoais estaduais e municipais: insegurança jurídica à vista? *Jota,* São Paulo, 3 dez. 2018. Disponível em: https://www.jota.info/especiais/pl-dados-sp-inseguranca-juridica-03122018. Acesso em: 11 nov. 2019.

LEVY, Heather Pemberton. Gartner's top 10 strategic predictions for 2017 and beyond: surviving the storm winds of digital disruption. *Gartner*, Stamford, 2016. Disponível em: <https://www.gartner.com/smarterwithgartner/gartner-predicts-a-virtual-world-of-exponential-change/. Acesso em: 4 out. 2019

LOBO, Ana Paula. LGPD: multa vai doer apenas no bolso de empresa brasileira. *Convergência Digital*, [S.l.], 2019. Disponível em: https://sis-publique.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=51554&sid=4. Acesso em: 25 nov. 2019

MARK Zuckerberg's Letter to Investors: 'The hacker way'. *Wired*, [S.l.], 2012. Disponível em: https://www.wired.com/2012/02/zuck-letter/. Acesso em: 1º out. 2019.

MEIER, Ricardo. Portas de plataforma da Linha 4-Amarela vão "interpretar" suas reações. *Metrô CTPM*, São Paulo, 16 abr. 2018. Disponível em: https://www.metrocptm.com.br/portas-de-plataforma-da-linha-4-amarela-vao-interpretar-suas-reacoes/. Acesso em: 3 out. 2019.

MELE, Christopher. Bid for access to Amazon Echo audio in murder case raises privacy concerns. *The New York Times,* New York, 2016. Disponível em: https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html. Acesso em: 5 out. 2019.

MICROSOFT. *Política de privacidade da Microsoft*. Albuquerque, Novo México, [2019]. Disponível em: https://privacy.microsoft.com/pt-br/privacystatement/. Acesso em: 12 mar. 2019.

MORAIS, Tarciso. Estações de metrô em SP com reconhecimento facial. *Renova Mídia, São Paulo,* 10 maio 2018. Disponível em: https://renovamidia.com.br/estacoes-de-metro-em-sp-com-reconhecimento-facial/. Acesso em: 3 out. 2019.

MURPHY, Margi. Amazon sends pharmacy stocks tumbling after snapping up online chemist. *Telegraph*, London, 2018. Disponível em: https://www.telegraph.co.uk/technology/2018/06/28/amazon-sends-pharmacy-stocks-tumbling-snapping-online-chemist/> Acesso em: 4 out. 2019.

NETBASE survey reveals consumers don't want brands listening to social

media conversations unless spoken to. *Netbase Quid*, Mountain View, CA, [2019]. Disponível em: https://www.netbase.com/press-release/netbase--survey-reveals-consumers-dont-want-brands-listening-to-social-media--conversations/. Acesso em: 3 out. 2019.

NETSHOES ligará para 2 milhões de clientes afetados por vazamento de dados. *Portal G1,* Brasília, DF, 28 fev. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/netshoes-ligara-para-2-milhoes-de-clientes-afetados-por-vazamento-de-dados.ghtml. Acesso em: 15 mar. 2019.

PAYÃO, Felipe. Michel Temer, finalmente, cria Autoridade de Proteção de Dados. *Tecmundo.* São Paulo, dez. 2018. Disponível em: https://www.tecmundo.com.br/seguranca/137510-michel-temer-cria-autoridade-protecao--dados-brasileiros.htm. Acesso em: 24 nov. 2019.

RIO DE JANEIRO. Ministério Público. *MPRJ entra com mandado de segurança para anular segredo de Justiça em ação contra Decolar.com*. Rio de Janeiro: Ministério Público do Estado do Rio de Janeiro, 2018. Disponível em: https://www.mprj.mp.br/home/-/detalhe-noticia/visualizar/61905. Acesso em: 3 out. 2019.

RODOTÀ, Stefano. *Uno statuto giuridico globale della persona elettronica.* Discurso proferido na 23ª Conferência Internacional sobre a Privacidade e a Proteção dos Dados Pessoais em Paris. 24 set. 2001. Disponível em: http://interlex.it/675/rodota5.htm. Acesso em: 11 nov. 2019.

SCHENKER, Jennifer. The Platform Economy. *The innovator.* 2019. Disponível em: http://tiny.cc/zkdf8y. Acesso em: 17 jun. 2019.

SILVA, Rafael. Multa de R$ 50 milhões será aplicada às empresas que não se adequarem à LGPD. *Canal Tech*, São Paulo, 10 out. 2019. Disponível em: https://canaltech.com.br/legislacao/multa-de-r-50-milhoes-sera-aplicada-as--empresas-que-nao-se-adequarem-a-lgpd-124552/. Acesso em: 24 nov. 2019.

SILVER, Curtis. How Facebook's 'people you may know' section just got creepier. *Forbes*, New York, 2016. Disponível em: https://www.forbes.com/sites/curtissilver/2016/06/28/how-facebooks-people-you-may-know-section-just-got-creepier/#5d78779e5f5a. Acesso em: 15 mar. 2019.

SMITH, Mitch. In Wisconsin, a Backlash Against Using Data to Foretell

Defendants' Futures. *The New York Times*, New York, 2016. Disponível em: https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against--using-data-to-foretell-defendants-futures.html?module=inline. Acesso em: 27 set. 2019.

SOPRANA, Paula. Deputados tentam derrubar decreto de Bolsonaro que cria cadastro base do cidadão. *Folha de São Paulo*, São Paulo, 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/10/deputados-tentam-derrubar-decreto-de-bolsonaro-que-cria-cadastro-do-cidadao.shtml. Acesso em: 29 nov. 2019.

STATT, Nick. Amazon sent 1,700 Alexa voice recordings to the wrong user following data request. *The Verge*, London, 2018. Disponível em: https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings--wrong-user-gdpr-privacy-ai. Acesso em: 5 out. 2019.

STOLTZ, Brenda. A new California Privacy Law could affect every U.S. business: will you be ready? *Forbes, New York,* 2019. Disponível em: https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy--act-could-affect-your-business/#79ab352436ac. Acesso em: 6 nov. 2019.

STUCKER, Kyle. 2 women killed in Farmington: one dover man on trial. *Fosters*, [Dover], 1 out. 2019. Disponível em: https://www.fosters.com/news/20191001/2-women-killed-in-farmington-one-dover-man-on-trial. Acesso em: 5 out. 2019.

TERMS of service; didn't read. Disponível em: https://tosdr.org/index.html?#. Acesso em: 19 jun. 2019.

VANDYSTADT, Nathalie. Regulamento Geral sobre a Proteção de Dados produz resultados, mas o trabalho deve prosseguir. *Comissão Europeia*, Comunicado de Imprensa, Bruxelas, 24 jul. 2019. Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/ip_19_4449. Acesso em: 12 nov. 2019.

WEISS, Debra Cassens. Chief Justice Roberts admits he doesn't read the computer fine print. *ABA Journal*, Chicago, [2019]. Disponível em: http://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_pripr. Acesso em: 25 jun. 2019.

WELCH, Chris. Apple completes Shazam acquisition, will make app ad-free for everyone. *The Verge, London,* 2018. Disponível em: http://tiny.cc/un2i8y. Acesso em: 19 jun. 2019.

WHATSAPP. *Informação Legal do Whatsapp.* Disponível em: https://www.whatsapp.com/legal/?lang=pt_br#privacy-shield. Acesso em: 29 maio 2019.

WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. *Portal G1,* São Paulo, jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 24 nov. 2019.

Vídeos, Filmes e Séries

HER. Direção: Spike Jonze, Produção: Megan Ellison, Spike Jonze e Vincent Landay. Estados Unidos: Warner Bros. Pictures, 2013.

INTERNETLAB. E quando te pedem informações pessoais em uma compra? São Paulo: *Internetlab*, 19 jul. 2018. 1 vídeo (168 min.). Disponível em: https://www.youtube.com/watch?v=uHZs3ADb6RQ. Acesso em: 25 set. 2019.

MATRIX. Direção: Lilly Wachowski, Lana Wachowski, Produção: Joel Silver. Estados Unidos, Austrália: Warner Bros. Pictures, 1999.

THIRTY SOUNDS GOOD. Q: the world's first genderless voice. [S.l.], 2018. Disponível em: http://www.thirtysoundsgood.dk/?flv_portfolio=q-the-worlds-first-genderless-voice. Acesso em: 4 out. 2019

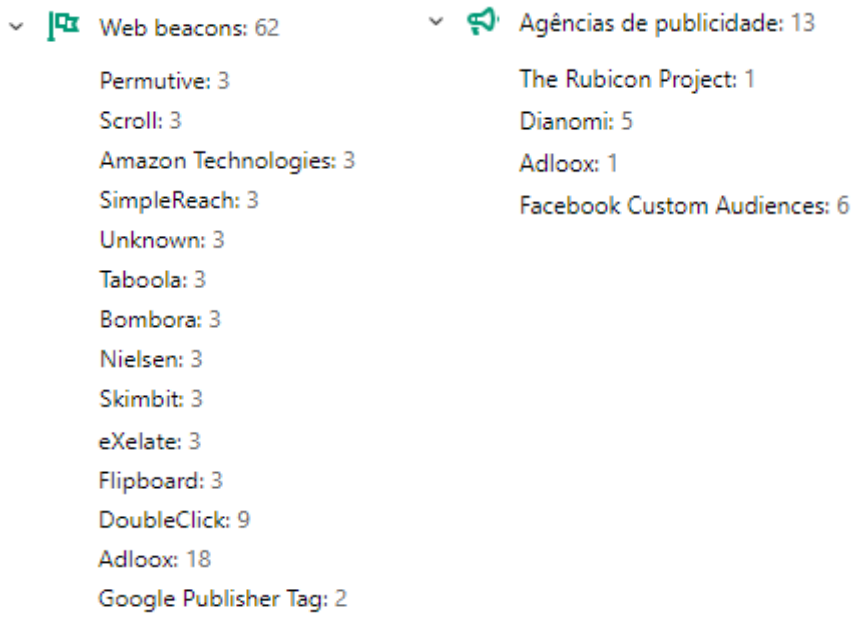
WESTWORLD. Produção de Jonathan Nolan e Lisa Joy. Los Angeles: Home Box Office; HBO, 2018.

APÊNDICE

Documentação de tentativa de coleta de dados da autora durante a visita à página <http://tiny.cc/xiidgz>, no dia 1º de outubro de 2019, às 22:04h. Utilizou-se a ferramenta paga de DNT do antivírus russo Kaspersky, eleito melhor antivírus de 2018 pela AV-TEST,[1] instituto de pesquisa em segurança de tecnologia alemão. No caso, tentou-se coletar dados por 91 vezes, sendo uma em rede social, 15 em análises da *web*, 62 em *web beacons* e 13 em agências de publicidade.

FIGURA 14 – TENTATIVAS DE RASTREIO DE DADOS EM FERRAMENTA DNT

1 AV-TEST. **AV-TEST Awards 2018 go to Kaspersky Lab**. 2019. Disponível em: <https://www.av-test.org/en/news/av-test-awards-2018-go-to-kaspersky-lab/>. Acesso em: 1º out. 2019.



Fonte: Elaborada pela autora.

PUBLICAÇÕES
DO CEJ