Universidade de Brasília – UnB

Faculdade de Direito – FD

Programa de Graduação em Direito

VIOLAÇÃO DE (CON)SENTIMENTOS:

Uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais

ISABELA DE ARAÚJO SANTOS

Brasília

2023

ISABELA DE ARAÚJO SANTOS

VIOLAÇÃO DE (CON)SENTIMENTOS:

Uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharela em Direito pelo Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD-UnB).

Orientadora: Professora Doutora ANA DE OLIVEIRA FRAZÃO VIEIRA DE MELLO

Brasília

2023

S

SANTOS, Isabela de Araújo
Violação de (con)sentimentos: Uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais / Isabela de Araújo SANTOS; orientador Ana de Oliveira Frazão Vieira de Mello. -- Brasília, 2023.
151 p.

Monografia (Graduação - Direito) -- Universidade de Brasília, 2023.

1. Proteção de dados pessoais. 2. Psicologia. 3. Manipulação comportamental. 4. Consentimento. 5. Violação. I. Frazão Vieira de Mello, Ana de Oliveira, orient. II. Título.

Citar como: SANTOS, Isabela de Araújo. *Violação de (con)sentimentos:* Uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais, 2023. 151 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

ISABELA DE ARAÚJO SANTOS

VIOLAÇÃO DE (CON)SENTIMENTOS:

Uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharela em Direito pelo Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD-UnB).

Aprovada em 13 de fevereiro de 2023

BANCA EXAMINADORA

_____

Professora Doutora **ANA DE OLIVEIRA FRAZÃO VIEIRA DE MELLO**
Faculdade de Direito da Universidade de Brasília (FD-UnB)
Orientadora – Presidente

_____

Psicóloga Doutora **CAROLINA DE RESENDE DAMAS CARDOSO**
Pró-Reitoria de Políticas Estudantis da Universidade Federal de Catalão (PRPE-UFCAT)
Examinadora

_____

Professor Doutor **BRUNO RICARDO BIONI**
Faculdade de Direito da Universidade de São Paulo (FD-USP)
Examinador

Brasília

2023

DEDICATÓRIA

Ao meu pai Francisco,

com eterno e imensurável amor

AGRADECIMENTOS

"Quando já não somos capazes de mudar uma situação - podemos pensar numa doença incurável, como um câncer que não se pode mais operar – somos desafiados a mudar a nós próprios."

VIKTOR FRANKL[1]

Quando li, pela primeira vez, a obra *Em Busca de Sentido*, de Viktor Frankl, no auge dos meus 19 anos, nunca pensei que esta frase acima transcrita faria – irônica ou poeticamente – tanto **sentido** na minha vida algum dia. Ao longo deste período da minha graduação na Universidade de Brasília, pude conviver e aprender com pessoas que me fizeram confirmar que o mais importante que levamos da vida é justamente poder contar com o apoio, a confiança e a ternura de quem esteve mais próximo de nós nas situações desafiadoras que podemos e, principalmente, nas que não podemos mudar.

Por isso, venho agradecer a algumas dessas pessoas que estiveram ao meu lado durante esses momentos, seja por terem me inspirado e motivado a trilhar o caminho que desejo, seja por terem me reerguido quando não consegui me levantar sozinha após tropeçar nos obstáculos da vida. Começarei meus agradecimentos por aqueles por quem sou grata pertencentes ao meio acadêmico, para então passar aos de âmbito mais intimista.

À Professora **Ana Frazão**, pela confiança depositada em minhas potencialidades como estudante e pesquisadora, desde o meu terceiro semestre, tendo se tornado uma grande fonte de inspiração para mim, como advogada, jurista e mulher. Sempre lembrarei com muita afeição dos ensinamentos que me passou e deixo registrada aqui minha gratidão pelas portas que me abriu.

Ao **Bruno Bioni**, pela oportunidade ímpar que me proporciona na Consultoria e pela bondade com que me trata. Você é um professor não apenas de proteção de dados e privacidade, mas também de generosidade e acolhimento. Desde que li seu primeiro livro, me tornei fã do

[1] FRANKL, Viktor. *Em Busca de Sentido:* um psicólogo no campo de concentração. 39ª ed., Petrópolis: Vozes, 2016, p. 137.

Bruno “acadêmico”, porém nunca imaginava que, um ano e meio depois, também me tornaria fã do Bruno “ser humano”.

À Professora **Carolina Cardoso**, por abrir meus olhos para a imensidão da Psicologia. Sem você, eu não teria escrito esta monografia e não teria chegado a conclusões que viriam a ser importantíssimas na minha vida, a exemplo da distinção de compaixão e empatia. Sou muito grata pelos nossos caminhos terem se cruzado nesta vida.

Ao Professor **Othon Lopes**, pela tamanha disposição e parceria ao longo dos últimos dois anos, bem como pela constante gentileza de suas palavras. À Professora **Gabriela Neves Delgado**, por me fazer acreditar na possibilidade de amor pela profissão e por fomentar minha criticidade de pensamento.

Ao Professor **Marcus Caldeira**, pela inspiração que gera não só em mim, mas em todos alunos e alunas que têm o privilégio de assistir às suas aulas, devido à sua postura como docente e sua afabilidade como pessoa. À Professora **Mônica Tiemy Fujimoto**, pelos ensinamentos em aula e no grupo de pesquisa; sendo uma inspiração para mim como pesquisadora e professora.

Aos meus amigos que a UnB me concedeu, **Elisa, Izabela, Natalie, Rodrigo, João, Tayná e Thiago**, pelos momentos únicos que apenas amizades verdadeiras podem proporcionar. Vocês são parte da minha história como estudante, pessoa e mulher; acho que jamais conseguirei expressar em palavras o quanto são importantes para mim.

Aos meus irmãos de outras mães, **Mariana, Gabrielle e Lucas**, por sempre me fazerem sentir compreendida, amada e respeitada, independentemente das minhas falhas como o ser humano imperfeito que sou. Vocês são a minha fonte de risos, sabedoria, reflexões e esperança de que o mundo pode se tornar, cada vez mais, um lugar melhor para viver.

À **família Santos,** em especial ao meu padrinho **Diomédio**, por me ensinar sobre a importância de batalhar pelos seus objetivos e sonhos, bem como de estar com as pessoas amadas nos momentos tortuosos da vida. À **família Araújo**, pela união, inclusão e pertencimento que permeia os laços afetivos entre todos, incluindo “agregados”. À **família Resende**, em especial à minha tia **Graça**, por me guiar, desde pequena, através de valores que me fizeram ser quem eu sou hoje.

Ao **André**, por ser o melhor irmão e o melhor amigo que eu poderia ter nesta vida. Realmente não sei o que seria de mim sem seus conselhos, sem sua perspectiva de vida, sem sua ajuda durante os pesadelos que vivenciamos. Você é o ser humano com o coração mais puro que conheço e eu não sei o que fiz para merecer tamanho privilégio de te ter. É um enorme prazer evoluir ao seu lado, dia após dia, errando e acertando, neste lindo desafio chamado vida.

À **Liliane**, por ser a mãe perfeita para mim (Deus foi cirúrgico na escolha). Por cada abraço, por cada lição, por cada conselho, por cada discordância, por cada música cantada em uníssono, por cada pensamento compartilhado, por cada angústia desabafada... Mãe, é um fato de que você veio para esta vida para ensinar mais do que para aprender (acho que absolutamente todos que te conhecem concordam comigo). Então, imagine o tamanho da minha gratidão por ser a sua aprendiz! Sua força e sensibilidade são admiráveis, e são a prova de que ambas qualidades não se excluem em alguém que possui inteligência emocional.

Enfim, ao meu pai **Francisco**, que partiu em decorrência de um câncer há exatamente um ano do dia que escrevo estes agradecimentos (14.01.2023). Sua trajetória de vida e morte é uma inspiração para mim e para muitas outras pessoas que pode influenciar durante seu caminho percorrido aqui na Terra, seja profissional ou pessoalmente. Obrigada por sempre ter acreditado em mim e por nunca ter deixado faltar amor na nossa família. Você foi a prova viva de que, mesmo passando pelo Inferno, podemos nos comportar como se estivéssemos no Céu.

RESUMO

O presente trabalho tem como escopo identificar quais as principais técnicas manipulatórias empregadas por entidades privadas para a extração sub-reptícia de dados pessoais de titulares. Além de averiguar as práticas ilícitas *per se* e as entidades privadas responsáveis por sua utilização, seu foco central é alicerçado em constatar como a manipulação comportamental afeta o campo decisório dos titulares de dados pessoais, repercutindo na livre manifestação de seus sentimentos, processos de cognição e consentimentos. Para tanto, o trabalho contou com métodos de pesquisa exploratória, documental, doutrinária e jurisprudencial; bem como se fundamentou em bases de dados relativas às áreas do Direto – especificamente Digital e Consumerista –, e da Psicologia – com enfoque na Behaviorista e Humanista. Diante disso, foi possível inferir que os titulares de dados encontram-se em posição de alarmante vulnerabilidade em face dos principais agentes econômicos que fazem uso de técnicas manipulativas para obter seus dados ilicitamente; tanto sob o aspecto psicológico de violação sentimental e cognitiva, quanto sob o prisma jurídico de inobservância ao consentimento livre, inequívoco e informado, estipulado pela legislação brasileira. Portanto, além de diagnosticar as principais consequências advindas pela utilização de técnicas manipulatórias contra titulares para a extração de seus dados, torna-se de suma relevância a proposta de medidas de salvaguardas e contravigilância capazes de empoderá-los suficientemente para que possam se proteger e monitorar quem os vigia no capitalismo de vigilância datificado.

Palavras-chave: Proteção de dados pessoais; Psicologia; Manipulação comportamental; Consentimento; Violação.

ABSTRACT

This thesis aims to identify the main manipulative techniques employed by private entities for the surreptitious personal data collection from data subjects. In addition to investigating the illicit practices *per se* and the private entities responsible for their use, its central focus is based on determining how the behavioral manipulation affects the personal data subject's decision process and how it affects their free expression of feelings, cognition processes and consent. To this purpose the thesis relied on exploratory, documentary, doctrinaire and jurisprudential research methods, as well as on databases related to the areas of Law - specifically Digital and Consumerism - and Psychology - with a focus on Behaviorism and Humanism. Thus, it was possible to infer that data subjects are in a position of alarming vulnerability in face of the main economic agents that use manipulative techniques to obtain their data illicitly; both under the psychological aspect of sentimental and cognitive violation, and under the legal prism of non-compliance with free, unambiguous and informed consent, stipulated by the Brazilian law. Therefore, besides diagnosing the main consequences arising from the use of manipulative techniques against data subjects for the illicit collection of their data, it becomes of utmost relevance the proposal of safeguards and counter-surveillance measures capable of empowering them sufficiently so that they can protect themselves and monitor who surveils them in the datified surveillance capitalism.

Keywords: Personal Data Protection; Psychology; Behavioral manipulation; Consent; Violation.

LISTA DE TABELAS

Tabela 1 – Técnicas de *neuromarketing* para análise do comportamento dos consumidores

Tabela 2 – Violações Jurídicas – *Dark Patterns*

Tabela 3 – Violações jurídicas – Captologia Comportamental

Tabela 4 – Violações Jurídicas – Predição Comportamental

Tabela 5 – Violações Jurídicas – Pesquisas de *neuromarketing*

Tabela 6 – Violações Jurídicas – Varejistas e birôs de crédito

LISTA DE FIGURAS

Figura 1: Situação real de cancelamento de inscrição em site

Figura 2: Situação real de cancelamento de inscrição em site

Figura 3: Situação real de cancelamento de inscrição em site

Figura 4: Situação real de *dark pattern nagging* em site

Figura 5: Situação real de *dark pattern nagging* em site

Figuras 6 e 7: Uma *dark pattern bait and switch* usualmente utilizada por companhias aéreas é bem exemplificada por estas duas imagens

Figura 8: Situação real de *dark pattern bait and switch* em site

Figura 9: Exemplo hipotético de interface de *dark pattern* de evasão em que usuários são encorajados a dispensar explicações, uma vez que é disponibilizada cobrindo o conteúdo principal do site

Figura 10: Exemplo hipotético de *dark pattern* de evasão em que é dada uma sobrecarga de informação técnica para titulares de dados a fim de obter seu consentimento com termos de uso ou políticas de privacidade de determinada plataforma ou *cookies*

Figuras 11 e 12: Caso concreto de *dark pattern* de evasão em que a interface para alteração de preferência de cookies impede o titular de dados de visualizar o conteúdo principal do site

Figura 13: Tríade de recompensas da terceira etapa do modelo do gancho

Figura 14: Modelo do gancho esquematizado

Figura 15: Correlação entre tipos de personalidade e fatores psicométricos, sendo as correlações relevantes $p < 1\%$, sendo p = Pearson Correlation

Figura 16: Variações de 22 expressões faciais em pessoas de cinco culturas distintas

Figura 17: A expressão “a”, com suas respectivas AUs, corresponde à emoção raiva; “b”, ao nojo; “c”, medo; “d”, à “alegria”; “e”, à tristeza; e “f” à surpresa

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

AUs – Unidades de Ação (*Action Units*)

CDC – Código de Defesa do Consumidor

CF – Constituição Federal da República Federativo do Brasil

EC – Emenda Constitucional

EDPB – *European Data Protection Board*

FIPPs – *Fair Informational Practice Principles*

GDPR – *General Data Protection Board*

HEW – *Department of Health, Education, and Welfare*

IoT – Internet das Coisas (*Internet of Things*)

LCP – Lei do Cadastro Positivo

LGPD – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

PETs – Privacy Enhancing Technologies

RIPD – Relatório de Impacto à Proteção de Dados Pessoais

Senacon – Secretaria Nacional do Consumidor

STJ – Superior Tribunal de Justiça

TICs – Tecnologias de Informação e Comunicação

SUMÁRIO

INTRODUÇÃO **15**

1 – SEÇÃO I – A VIOLAÇÃO DE SENTIMENTOS **18**

CAPÍTULO 1 – O CAPITALISMO DE VIGILÂNCIA DATIFICADO: MUDANÇA PARADIGMÁTICA, CARACTERÍSTICAS E RISCOS **21**

CAPÍTULO 2 – ENTIDADES PRIVADAS VIGILANTES: OS PRINCIPAIS ATORES RESPONSÁVEIS PELA EXTRAÇÃO DE DADOS PESSOAIS E PELO SEU CONSEQUENTE FEEDBACK LOOPING (POSITIVO E NEGATIVO) **28**

2.1 - PLATAFORMAS DIGITAIS E BIG TECHS: DEFINIÇÕES, ESFERAS DE PODER E ASSIMETRIA INFORMACIONAL 28

2.2 – DEMAIS ATORES ECONÔMICOS DO MUNDO DIGITALIZADO: EMPRESAS VAREJISTAS, BIRÔS DE CRÉDITOS E WEBSITES DE COMPANHIAS DE OUTROS RAMOS ECONÔMICOS 32

CAPÍTULO 3 – TÉCNICAS MANIPULATÓRIAS UTILIZADAS CONTRA TITULARES DE DADOS **36**

3.1 – A ECONOMIA COMPORTAMENTAL: (HIPER)NUDGES, DARK PATTERNS E DISSONÂNCIA COGNITIVA 36

3.2 – A ECONOMIA PSÍQUICA DOS ALGORITMOS: MODELO DO GANCHO, PSICOMETRIA E MATEMATIZAÇÃO DE EXPRESSÕES FACIAIS 51

3.2.1 – Matriz captológica *52*

3.2.2 – Matriz preditiva *58*

3.3 – A NEUROCIÊNCIA: NEUROMARKETING, PESQUISAS INVASIVAS E APRIMORAMENTO DA MANIPULAÇÃO 63

SEÇÃO II – A VIOLAÇÃO DE CONSENTIMENTOS **73**

CAPÍTULO 4 – O ARCABOUÇO JURÍDICO DE PROTEÇÃO AOS TITULARES DE DADOS **75**

4.1 – O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: BREVE PANORAMA HISTÓRICO, DESVINCULAÇÃO DO DIREITO À PRIVACIDADE E DUPLA FUNÇÃO VINCULANTE 75

4.2 – A LEI GERAL DE PROTEÇÃO DE DADOS: PRINCÍPIOS NORTEADORES, BASES LEGAIS E DADOS PESSOAIS (SENSÍVEIS E NÃO SENSÍVEIS) 80

4.3 – O CONSENTIMENTO: MOTIVOS DE SUA APLICAÇÃO, ADJETIVAÇÕES DA LGPD E DIÁLOGO COM O GDPR 90

4.3.1 – O consentimento livre *92*
4.3.2 – O consentimento informado *94*
4.3.3 – O consentimento inequívoco *97*
4.3.4 – O consentimento específico *99*
4.4 – O CÓDIGO DE DEFESA DO CONSUMIDOR E O MARCO CIVIL DA INTERNET: VULNERABILIDADE DO CONSUMIDOR-CIDADÃO, DIÁLOGO DE FONTES E DADOS CADASTRAIS 100
CAPÍTULO 5 – ANÁLISE JURÍDICA DAS PRÁTICAS MANIPULATÓRIAS 106
5.1 – CONFIGURAÇÃO DA ILICITUDE DE DARK PATTERNS E SUAS AMEAÇAS AOS DIREITOS DOS TITULARES DE DADOS PESSOAIS 106
5.2 – MODELO DO GANCHO E MATEMATIZAÇÃO DAS EXPRESSÕES FACIAIS COMO VIOLAÇÕES AO CONSENTIMENTO DOS TITULARES 109
5.2.1 – Práticas sub-reptícias da captologia comportamental *109*
5.2.2 – Práticas sub-reptícias da predição comportamental *113*
5.3 – A ILICITUDE DE PESQUISAS DE NEUROMARKETING 117
5.4 – VIOLAÇÕES DE OUTROS SETORES ECONÔMICOS: EMPRESAS VAREJISTAS E BIRÔS DE CRÉDITO 121
CAPÍTULO 6 – PROPOSTAS DE REFORÇO DE SALVAGUARDAS E CONTRAVIGILÂNCIA 126
6.1 – MEDIDAS DE ACCOUNTABILITY E ENFORCEMENT: ANPD E SENACON COMO ATORES CENTRAIS DE UMA GOVERNANÇA MULTISSETORIAL 127
6.2 – FERRAMENTAS DE CONTRAVIGILÂNCIA: COMO OBTER TRANSPARÊNCIA EM UM MUNDO DIGITAL OPACO 137
CONCLUSÃO 141

INTRODUÇÃO

"Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso, vamos perceber o universo inteiro como um fluxo de dados, considerar organismos pouco mais que algoritmos bioquímicos e acreditar que a vocação cósmica da humanidade é criar um sistema universal de processamento de dados – e depois fundir-se a ele."

YUVAL HARARI[2]

A reflexão acima transcrita do filósofo Yuval Harari traz duas considerações relevantes para a sociedade contemporânea: a primeira refere-se à existência humana hoje estar condicionada a um fluxo de dados; e a segunda, ao poder que esses dados possuem sobre os humanos. Tal relação simbiótica conferida pela inovação tecnocientífica gera repercussões em diversas searas da vida social, incluindo o Direito e a Psicologia, visto que a extração ilícita de dados pessoais por parte de agentes econômicos pode interferir em seus processos cognitivos e decisórios, afetando suas emoções e infringindo seus direitos.

Essa correlação entre ambas as áreas de estudo torna-se ainda mais evidente especialmente a partir do momento em que são averiguadas técnicas manipulativas para a obtenção de dados pessoais de titulares enquanto cidadãos em uma ordem democrática de direito. Ainda mais porque há de se considerar até que ponto a liberdade de escolha no mundo datificado ainda existe, diante do emprego de práticas psicológicas persuasivas que veem o indivíduo como nada mais que mero cobaia experimental.

Nesse sentido, este trabalho tem como **objetivo central** se propor a identificar quais são as principais[3] técnicas manipulatórias comportamentais empregadas por entidades privadas para a extração ilícita de dados pessoais de titulares passíveis de violar tanto seus sentimentos e processos cognitivos, quanto seus consentimentos. Para isso, os **objetivos específicos** que se

[2] HARARI, Yuval Noah. *21 lições para o século 21.* São Paulo: Companhia das Letras. Edição do Kindle, p. 60.
[3] Não há a pretensão, neste trabalho, de se mapear todas as técnicas manipulatórias existentes, mas sim de apresentar os principais métodos manipulativos averiguados a partir da metodologia escolhida.

pretende alcançar, por meio de uma **metodologia** que abrange a análise de pesquisa exploratória e documental interdisciplinar,[4] são:

i) Caracterizar os principais agentes econômicos privados que se utilizam de técnicas sub-reptícias para obter dados ilicitamente de titulares;

ii) Constatar quais são as violações, segundo as legislações vigentes, aos direitos dos consumidores-titulares ocasionadas por tais agentes econômicos;

iii) Avaliar como o ordenamento jurídico brasileiro confere salvaguardas aos cidadãos, enquanto titulares e consumidores, contra as práticas ilícitas manipulativas empregadas pelas entidades privadas;

iv) Propor mecanismos de defesa práticos para os titulares contra a manipulação das entidades privadas, sob a óptica da regulação – *ex ante* e *ex post* – e do engajamento dos próprios titulares de dados; e

v) Comparar a concepção "psico-orientativa" de indivíduo dada pelos agentes privados manipuladores e a concedida pelo ordenamento jurídico brasileiro, caso divergentes.

A **justificativa** para tais objetivos surge porquanto, ao definir por quem e quais técnicas são empregadas para manipular titulares de dados pessoais, é possível estabelecer o nível de proteção que as normas jurídicas conferem para ampará-los em situações de vulnerabilidade – seja por estarem configurados em polos de assimetria informacional, seja por se encontrarem em relações de consumo. Diante disso, a sugestão de medidas de contravigilância advém como impulso interessante para empoderar os titulares em relação a seu poder decisório e incentivar atores regulatórios a atuarem em sua defesa.

A **hipótese** levantada, ao menos *prima facie*, é a de que há uma manipulação massiva de titulares de dados por entidades privadas nos dias atuais e que o ordenamento jurídico brasileiro é capaz de tutelar os direitos do consumidor e do titular de dados submetidos a técnicas manipulatórias comportamentais empregadas por tais agentes manipuladores.

Para corroborar ou refutar tal hipótese, o trabalho contará com a análise minuciosa de **marco teórico** relativo, em um primeiro momento, à Filosofia Moderna e Contemporânea,[5] e

[4] **Foram analisadas bases de dados documentais, doutrinárias, legislativas e jurisprudenciais referentes às áreas do Direito Civil, Digital, Consumerista, Concorrencial e Constitucional; bem como documentos, artigos e livros da Psicanálise Freudiana, do Behaviorismo, da Psicologia Cognitiva e do Humanismo**.

[5] A exemplo de Michel Foucault e Byung-Chul Han, respectivamente.

à Psicologia Comportamental[6] – especificamente trazendo referências bibliográficas do *Behavioral Economics*, da Economia Psíquica dos Algoritmos e da Neurociência[7] para identificar as entidades privadas manipuladoras, bem como para compor o entendimento da violação dos processos cognitivos e dos sentimentos dos titulares de dados expostos à manipulação comportamental. E, em um segundo momento, esta monografia abordará a violação de consentimentos a partir da leitura doutrinária, legislativa, histórica e jurisprudencial de marcos teóricos relevantes do campo do Direito Civil, Consumerista, Digital – especificamente em relação à proteção de dados pessoais – e Constitucional.[8] Por fim, vale ressaltar que, caso viável, pretende-se realizar a comparação entre as concepções de indivíduo conferidas pelas entidades privadas e pelo ordenamento jurídico a partir do paralelismo paradigmático da Psicologia Behaviorista e da Humanista.[9]

Com isso, eis o trabalho de conclusão de curso *Violação de (con)sentimentos: uma análise psicojurídica da vulnerabilidade de titulares de dados diante de técnicas manipulatórias comportamentais*, cuja estrutura será dividida em duas seções: a primeira relativa à violação de sentimentos e capacidades cognitivas, e a segunda, de consentimentos.

[6] Principalmente baseando-se nas obras de B.F. Skinner.
[7] Tais como: Daniel Kahneman, Cass Sunstein e Richard Thaler; Michal Kosinski, Lewis Goldberg e Lisa Barret; e Monica Bercea, respectivamente.
[8] Stefano Rodotà, Ana Frazão e Gustavo Tepedino; Claudia Lima Marques e Bruno Miragem; Danilo Doneda, Laura Schertel Mendes e Bruno Bioni; Ingo Wolfgang Sarlet e Ronald Dworkin, respectivamente. Bem como legislações referentes a cada área, como a Lei do Cadastro Positivo, o Código de Defesa do Consumidor, a Lei de Proteção de Dados, o Marco Civil da Internet e a Constituição Federal.
[9] Especificamente dos postulados de Abraham Maslow e Carl Rogers.

1 – SEÇÃO I – A VIOLAÇÃO DE SENTIMENTOS

"As tecnologias oferecem um enorme potencial, e não é exagero referir-se às oportunidades decorrentes da sociedade da informação. [...] Na maioria dos aspectos da vida cotidiana, os cidadãos são hoje obrigados a utilizar as novas tecnologias para não serem social e economicamente marginalizados. Porém as novas tecnologias também trazem consigo um potencial de perigos: não só o de terceiros, incluindo o Estado, penetrando na esfera privada, mas também o desenvolvimento de um poder de comunicação e econômico que impõe seus interesses seletivamente através da manipulação [...]."

WOLFGANG HOFFMANN-RIEM[10]

Tal como relatado por Wolfgang Hoffmann-Riem, a sociedade contemporânea depara-se com múltiplos desafios decorrentes do desenvolvimento tecnocientífico. Enquanto há uma coerção velada aos indivíduos de engajamento em suas relações interpessoais mediadas pela internet, existem concomitantemente atores públicos e privados se beneficiando dessa norma de conduta social imposta aos cidadãos; vigiando-os e manipulando-os.

O escopo desta seção é elucidar quem são os mencionados atores vigilantes do setor privado, bem como quais são as técnicas por eles utilizadas para manipular os indivíduos, incluindo seus sentimentos e emoções. Todavia, antes de mais nada, vale pontuar a definição do que seriam sentimentos e emoções, de acordo com algumas das teorias da Psicologia que serão abordadas neste trabalho.

[10] Tradução livre: "Las tecnologías ofrecen enormes potencialidades, y no es ninguna exageración hacer referencia a las oportunidades que se derivan de la sociedad de la información. En la mayoría de los aspectos de la vida cotidiana, los ciudadanos están hoy obligados a utilizar las nuevas tecnologías si no quieren quedar social y económicamente marginados. Pero las nuevas tecnologías comportan también un potencial de peligros: no sólo el de que terceros, incluido el Estado, penetren en el ámbito privado, sino también el desarrollo de un poder de comunicación y económico que imponga sus intereses de forma selectiva mediante la manipulación [...]". – HOFFMANN-RIEM, Wolfgang. *Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información*, ReDCE, n. 22, 2014, p. 49.

Para a Psicanálise Freudiana, os sentimentos e as emoções são definidos como fenômenos mentais, abstratos, e estariam alojados em um local "oculto da mente humana".[11] Logo, se algum fato provocar irritação em um indivíduo, gestos de raiva e agressividade seriam manifestados publicamente, advindos desse lugar onde estariam anteriormente reprimidos.[12] Apesar de não desconsiderarmos a relevância dessa conceituação, principalmente por se valer da concepção da existência da mente humana, bem como de manifestações conscientes e inconscientes advindas dela, outra base teórica também fundamentará a compreensão do presente trabalho, por melhor delinear a atuação de vigilância massiva de empresas contra consumidores, enquanto titulares de dados pessoais.

A Psicologia Behaviorista de Skinner[13] conceitua os sentimentos e as emoções como manifestações corporais concretas do organismo,[14] ou seja, ações sensoriais, como ouvir e ver,[15] influenciadas por circunstâncias externas. Isso porque o Behaviorismo é a área da Psicologia voltada para o estudo do comportamento humano, visando a sua previsão, controle e manipulação. Logo, a análise experimental do comportamento, por meio de operações emocionais,[16] favoreceria a compreensão dos sentimentos e das emoções, justamente por esclarecer os papéis que o ambiente exerce sobre o indivíduo.[17]

Não é por outro motivo que, como será apresentado adiante (especificamente no capítulo 3), empresas – como plataformas digitais e *big techs* – passaram a investir grande parte de seu capital em tecnologias capazes de analisar e prever a tomada de decisão de seus consumidores,

---

[11] A explicação é de: GUILHARDI, Hélio J. *Auto-estima, autoconfiança e responsabilidad*e, Instituo TCR, Orgs.: Maria Zilah da Silva Brandão, Fatima Cristina de Souza Conte, Solange Maria B. Mezzaroba. Santo André, SP: ESETec Editores Associados, 2002, p. 1.

[12] Sigmund Freud, precursor da Psicanálise, denominou o local de repressão de emoções de "Id", bem como estabeleceu que os adoecimentos psíquicos se dariam justamente pela exteriorização anormal das emoções contidas no Id: "Tinha-se de admitir que a doença se instalava porque a emoção desenvolvida nas situações patogênicas não podia ter exteriorização normal; e que a essência da moléstia consistia na atual utilização anormal das emoções 'enlatadas'." – FREUD, Sigmund. Cinco lições de psicanálise, In: *Obras Psicológicas Completas de Sigmund Freud*, XI. Imago, 1910, p. 14.

[13] Toma-se aqui como ponto de partida a concepção behaviorista de Skinner, que considera a relevância das emoções para a análise do comportamento. – *Cf:* SILVEIRA, Heitor Vicente da et al. Usos do termo emoção na obra de B. F. Skinner. Acta Comportamentalia, *Revista Latina de Análise de Comportamiento*, v. 27, n. 4, 2019.

[14] *Idem.*

[15] SKINNER, Burrhus F. O lugar do sentimento na análise do comportamento. In: *Questões recentes na análise comportamental*. Campinas, SP: Papirus. Cap. 1, 1991.

[16] As operações emocionais são mudanças ambientais que criam os chamados "estados emocionais", ou seja, alteração imediata e temporária da força dos comportamentos de um repertório de um indivíduo (o que pode resultar em alta probabilidade de ocorrência de uma resposta e baixa probabilidade de outra) – SILVEIRA et al. *Op. cit*., 2019, p. 486.

[17] *Idem.*

bem como naquelas aptas a captar a sua atenção, ao realizar pesquisas relativas à manipulação de seus sentimentos e suas emoções, bem como de seus processos cognitivos – o que impacta diretamente suas tomadas de decisões.

Assim, partindo das definições e teorias apresentadas, passemos a examinar o contexto de surgimento da sociedade da informação, mencionada por Wolfgang Hoffmann-Riem, caracterizada pela existência de vigilantes e vigiados.

CAPÍTULO 1 – O capitalismo de vigilância datificado: mudança paradigmática, características e riscos

No clássico *Vigiar e Punir: história da violência nas prisões*[18], Michel Foucault descreve a chamada "sociedade disciplinar" como aquela estruturada por "sujeitos da obediência"[19], que, dentro de muros de instituições disciplinares, sentem-se coagidos a se comportarem de maneira regrada sob uma vigilância hierárquica e uma ameaça de sanção normalizadora. Para Byung-Chul Han, a sociedade disciplinar é dominada pela noção de negatividade,[20] isto é, de proibição advinda de mandamento ou lei, o que consumaria o denominado panóptico de Bentham.

Esse conceito, cunhado pelo filósofo e jurista inglês Jeremy Bentham, no século XVIII, descreve um modelo de penitenciária ideal, em que todos inseridos no sistema podem ser vigiados – sem nem mesmo terem a ciência disso –, o que repercutiria em uma modulação comportamental parametrizada ideal. Segundo Foucault, o panóptico seria compreendido como um modelo generalizável para a definição das relações de poder da "vida cotidiana dos homens"[21]. Logo, panóptico de Bentham pode servir de analogia para as estruturas de poder analisadas por Foucault, o qual constatou que, desde o século XVII, se manifestam não mais através do "poder do soberano sobre a morte"[22], e sim a partir do "biopoder".[23]

O biopoder se anuncia como o "estímulo, [o] fortalecimento, [o] controle, [a] vigilância, [o] aumento e [a] organização das forças sujeitadas".[24] Han adiciona que sua interferência nos indivíduos de uma sociedade ocorre em "processos e leis biológicas pelos quais a população é

---

[18] FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão, 27ª ed., Petrópolis: Vozes, 1999.

[19] Ambos os termos "sociedade disciplinar" e "sujeitos da obediência" remetem à obra *Sociedade do Cansaço*, de Byung-Chul Han, que esmiuça a visão do capitalismo moderno industrial de Michel Foucault. Vide: HAN, Byung-Chul. *Sociedade do Cansaço*, 2ª ed. ampliada, Petrópolis, RJ: Vozes, 2017, p. 23.

[20] *Ibid.*, p. 24.

[21] FOUCAULT. *Op. cit.*, p. 228.

[22] Neste ponto, fazemos referência à ideia que Foucault traz em sua obra de que o panóptico revela uma nova proposta advinda com a tecnologia política: a vigilância como forma de evitar conduta ilícitas, em detrimento das punições monárquicas custosas e inúteis, denominadas "superpoder monárquico" – *Ibid.*, p. 348.

[23] Tanto o "poder soberano sobre a morte", quanto o "biopoder" são conceitos extraídos da obra *No Enxame: perspectivas do digital* utilizados a fim de se fazer uma aferência entre diferentes modalidades de poder ao longo através do tempo, considerando as mudanças paradigmáticas ocorridas principalmente entre os séculos XVII e XIX. Vide: HAN, Byung-Chul. *No exame*: perspectivas do digital, Petrópolis, RJ: Vozes, 2018, p. 129.

[24] FOUCAULT, Michel. *A vontade de saber*: Sexualidade e verdade I. Frankfurt a. M., 1977, p. 163.

guiada e conduzida",[25] não havendo influência direta em sua *psique* – isto é, na subjetividade, personalidade e consciência de cada indivíduo.[26]

A mudança paradigmática[27] ocorrida nos séculos XX e XXI, proporcionada com o aprimoramento das Tecnologias de Informação e Comunicação (TICs), revela o surgimento da sociedade do desempenho,[28] em detrimento da disciplinar. No lugar da negatividade característica do modelo anterior, passa a ter espaço a positividade, a iniciativa e a motivação.[29] Com fins de maximizar a produtividade, o sistema econômico, alicerçado agora na psicopolítica e no psicopoder[30] – passando a adentrar o inconsciente coletivo digital[31] e o campo volitivo das massas –, impulsiona os sujeitos a oprimirem a si mesmos[32] para alcançarem a obediência e o êxito superprodutivo.

O panóptico digital, cuja denominação foi cunhada por Han para suceder o paradigma anterior, concede aos indivíduos uma falsa sensação de liberdade,[33] pois a sua "hiperatividade",[34] estimulada pela violência sistêmica de desempenho, produz os chamados

---

[25] HAN. Op. cit., 2018, p. 129.

[26] Utilizamo-nos aqui, para fins elucidativos, a Teoria Humanista da Psicologia para a definição de "psique", que considera a concepção de sujeito em sua subjetividade interior, individual e autoconsciente, sempre voltada, em última instância, para sua autorrealização. – JACÓ-VILELA, Ana Maria; FERREIRA, Arthur Arruda Leal; PORTUGAL, Francisco. *História da psicologia*: rumos e percursos, Rio de Janeiro: Nau Editora, 2006, p. 336.

[27] Adotamos aqui a nomenclatura "mudança paradigmática" para nos referirmos à hermenêutica adotada por Thomas Kuhn em *A estrutura das revoluções científicas* para caracterizar as revoluções científicas, também denominadas mudança de paradigma: "episódios de desenvolvimento não-cumulativo, nos quais um paradigma mais antigo é total ou parcialmente substituído por um novo, incompatível com o anterior" – KUHN, Thomas S. A estrutura das revoluções científicas, 5ª edição, São Paulo: Editora Perspectiva, 1998, p. 126.

[28] HAN. Op. cit., 2017, p. 23.

[29] *Ibid.*, p. 24.

[30] A psicopolítica, de acordo com Han, seria a possibilidade de interpretar modelos comportamentais com o advento do Big Data. Vide: HAN. *Op. cit.*, 2018, p. 130.

[31] No capítulo intitulado Psicopolítica, do livro *No Enxame: perspectivas do digital*, Han descreve a nova ordem econômica do panóptico digital como aquela fundada na transparência política e no controle de pensamentos, pela sua capacidade de adentrar o "inconsciente-coletivo", também denominado "inconsciente digital": "O psicopoder é mais eficiente do que o biopoder na medida em que vigia, controla e influencia o ser humano de dentro para fora" – *Ibid*., pp. 129-134.

[32] Han descreve a **autoexploração** como um sistema eficiente, visto caminhar de mãos dadas com a falsa sensação de liberdade: "O sujeito de desempenho explora a si mesmo, até consumir-se completamente". – HAN. *Op. cit*., 2017, p. 101.

[33] SANTOS, Isabela de Araújo; ARAÚJO, Tayná Frota de. Liberdade, previsão, ação: desafios da Lei de Liberdade Econômica sob o viés da Economia Comportamental. In: FRAZÃO, Ana; PRATA DE CARVLHO, Angelo. *Lei de Liberdade Econômica*: análise crítica, 1ª ed., Rio de Janeiro: Forense, 2022, p. 141.

[34] A hiperatividade aqui mencionada é um sinônimo da "massificação do positivo" para o alcance da melhor performance econômica enquanto sujeito do sistema capitalista – HAN, *Op. cit.*, 2017, p. 21.

"infartos psíquicos".[35] Dessa forma, o "hipercapitalismo"[36] subjuga as relações humanas em relações de mercado e normaliza a histeria pela sobrevivência,[37] transvestida em uma busca incessante por capital.

Além das questões relacionadas à suposta falta de soberania dos sujeitos sobre suas escolhas – que serão tratadas adiante no capítulo 3 – cabe ressaltar, neste momento, que a vigilância descrita por Foucault como hierárquica e punitiva, para caracterizar a sociedade pré-moderna, hoje se converteu em uma vigília mais sutil e, a princípio, menos ameaçadora sob as lentes de quem é vigiado, **apesar de apresentar-lhe riscos significativos sob o ponto de vista psicológico e jurídico**.

A atual conformação socioeconômica, fundada em uma monetização da informação extraída de dados pessoais, configura um cenário denominado **capitalismo de vigilância**, que, segundo Shoshana Zuboff[38] e Frank Pasquale,[39] caracteriza o modelo econômico contemporâneo de monitoramento e vigília constantes sobre cada passo da vida dos cidadãos, seja pelos seus governos, seja pelo setor privado da economia.

Esse sistema de mercantilização e comoditização[40] dos dados permite uma redistribuição do poder na era da informação. Considerando que a comunicação constitui historicamente uma fonte primordial de poder, a era do capitalismo dos dados[41] associa tecnologias em rede aos benefícios sociais e políticos do mundo *online*, podendo resultar em narrativas utópicas tecnológicas[42] ou em dominações assimétricas, constituindo o chamado *one-*

---

[35] Os infartos psíquicos, segundo Han, decorrem do imperativo de desempenho como um novo mandato da sociedade pós-moderna do trabalho. Como consequência disso, o próximo estágio da autoexploração do sujeito seria o *burnout* e, em seguida, a depressão – pela falta de consciência de conflito intrapsíquico, decorrente de um sistema socioeconômico que estimula identidades flexíveis e não duradouras. – *Ibid.*, pp. 27 e 97.

[36] *Ibid.*, p. 127.

[37] Sobre a histeria pela sobrevivência, o autor enuncia que o hipercapitalismo se nutre da ideia de que quanto mais capital, mais vida é gerada. Isso geraria mais capacidade para se viver e, por isso, a histeria pela busca incessante de mais capital. Vide: *Ibid.*, p. 107.

[38] ZUBOFF, Shoshana. em: *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

[39] PASQUALE, Frank. *The black box society*. The secret algorithms that control money and information, Cambridge: Harvard University Press, 2015.

[40] O vocábulo "comoditização" é empregado por Thomas Law em: LAW, Thomas. *A Lei Geral de Proteção de Dados:* uma análise comparada ao novo modelo chinês, 1ª ed., Belo Horizonte, São Paulo: D'Plácido, 2021, p. 33.

[41] Outra nomenclatura usual para caracterizar o modelo econômico contemporâneo – *Ibid*., p. 35.

[42] CASTELLS, Manuel. Communication, power and counter-power in the network society. *International journal of communication*, v.1, n.1, 2007, pp. 238-266.

way mirror[43] – a partir de práticas de vigilância unilaterais daqueles que detêm o monopólio do processamento dos dados.

É nesse diapasão que Shoshana Zuboff postula que, no capitalismo de vigilância, os lucros derivam da acumulação de traços digitais, a partir da vigília unilateral, e da modificação do comportamento humano.[44] Com isso, as próprias relações sociais são drasticamente modificadas pela mediação das novas tecnologias, bem como as concepções e usos das autoridades e do poder,[45] afinal, a partir do momento em que se torna possível adentrar a *psique* humana, há a possibilidade de influenciar consciências[46] e opiniões dos mais diversos cunhos: políticos, morais, religiosos e sociais.

Logo, na medida em que os dados pessoais foram se tornando cada vez mais fontes de informações úteis para a constituição de poder socioeconômico, empresas de diferentes setores de produção tiveram de se adaptar ao novo contexto de relações de oferta e demanda baseado em *Big Analytics*, ou seja, na análise de correlações, diagnósticos, padrões de inferências e associações[47] a partir do processamento de dados.

Surge daí a necessidade de **diferenciar conceitualmente "dado" de "informação**". Apesar de recorrentemente utilizados como sinônimos, dado é o estado primitivo da informação,[48] isto é, o conjunto de "fatos brutos"[49] que, a partir do seu tratamento, podem ser convertidos em informação. Esta última, logo, seria o que pode ser deduzido de inteligível do primeiro.[50]

Assim, pode-se inferir dessas definições que os dados e a capacidade de processá-los, a fim de convertê-los em informações úteis, guardam uma relação de interdependência entre si,

---

[43] Como pontua Frank Pasquale, os dados pessoais são utilizados por governos e grandes *players* econômicos para a criação da prática denominada *one-way mirror*, garantindo que tais agentes saibam tudo dos cidadãos, enquanto estes nada saibam daqueles. Essa prática seria operacionalizada a partir de sistemas de monitoramento e vigília constantes da vida cotidiana dos cidadãos, constituindo a chamada sociedade de vigilância. – PASQUALE. *Op. cit.*, 2015, pp. 9-45.

[44] ZUBOFF, Shoshana. The secrets of surveillance capitalism, *Frankfurter Allgemeine Zeitung*, 2016.

[45] ZUBOFF, Shoshana. Big Other: surveillance capitalism and prospects of an information civilization. *Journal of Information Technology*, v.30, n.1, pp. 75-89, 2015, p. 77.

[46] WU, Tim. *The attention merchants*: the epic scramble to get inside our heads. New York, Kopf, 2016.

[47] Conceito baseado em: FRAZÃO, Ana. Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência. In: *Empresa, Mercado e Tecnologia*, 2019, p. 182.

[48] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 152.

[49] BIONI, Bruno Ricardo. *Proteção de dados:* a função e os limites do consentimento, 3ª ed., Rio de Janeiro: Forense, 2021, p. 32.

[50] *Idem.*

só fazendo sentido em concomitância, visto que "a geração de valor depende do acesso simultâneo aos dois recursos",[51] não podendo ser isolados em uma análise jurídica de uma ordem econômica fomentada por um constante fluxo de dados.

A maneira como esse fluxo de dados teve sua coleta, armazenamento, transferência, acesso e descarte otimizados tem intrínseca relação com o advento do *Big Data*[52] e do *Big Analytics*, os quais proporcionaram maior **velocidade, valor, variedade e volume aos dados**.[53] Esse aprimoramento do processamento de dados incentiva, de modo diretamente proporcional, o aumento da vigilância, visto a relevância das informações extraídas deles para economia contemporânea.

Somando-se essas tecnologias à capacidade de algoritmização desses dados para o desenvolvimento de produtos e serviços personalizados a consumidores e titulares de dados, o poder econômico daqueles que os processam torna-se díspar dos que não o possuem. Nesse sentido, insta salientar que a indústria de *Marketplace*, ao desenvolver produtos e serviços de Internet das Coisas (IoT),[54] permite a hiperconexão entre pessoas e coisas em qualquer lugar e em qualquer momento.[55] Esse avanço tecnológico, portanto, tem um potencial significativo nas modificações do comportamento, bem como na abrangência dos tipos de dados que são coletados de seus consumidores.

Isso porque "os dados coletados pelos dispositivos inteligentes de IoT podem conter dados pessoais muito sensíveis com base no tipo de aplicativo e fontes de dados"[56]. Ademais,

---

[51] FRAZÃO, *Op. cit*., 2019, p. 182.

[52] O *Big Data* não possui uma definição uníssona na doutrina, porém adotamos aqui o conceito de Ana Frazão, que o caracteriza pela presença de velocidade, veracidade, variedade e volume no processamento de dados – FRAZÃO, Ana. Fundamentos da proteção de dados pessoais: Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*, São Paulo: Revista dos Tribunais, Thomson Reuters, 2019, p. 25.

[53] Os chamados 4V's do Big Data garantem que o grande e diversificado volume de dados gere, rapidamente, valor à informação útil extraída dele, a partir do *Big Analytics*. – HASHEM, Ibrahim et al. The rise of "big data" on cloud computing: review and open research issues. *Information systems*. v. 47, pp. 98-115, 2015.

[54] A abreviação IoT remete às palavras em inglês *Internet of Things*. A IoT é o processo de atribuição de funções de conexão à internet a objetos e aparelhos físicos diariamente utilizados, capazes de suportar tal interação comunicacional – por exemplo, aqueles de identificação por radiofrequência, sensores sem fio ou nanotecnologia. Vide: MAGRO, Américo Ribeiro. A (In)eficácia do direito à anonimização de dados pessoais em face da análise de big data dos metadados produzidos no âmbito da internet das coisas. In: TEIXEIRA, Tarcísio (coord.). *Proteção de dados*, São Paulo: Editora Jvspodium, 2020, pp. 13-55.

[55] LAW, *Op. cit*., 2021, p. 53.

[56] *Ibid*., p. 55.

os fornecedores de produtos e serviços de IoT costumam buscar a confiança do consumidor,[57] o que, por vezes, repercute em violações de consentimento de titulares de dados pessoais.

No que concerne ao consentimento dos titulares de dados – cuja compreensão será aprofundada no subcapítulo 4.3 –, a legislação brasileira, após a promulgação e vigência da Lei Geral de Proteção de Dados (LGPD), em 2018, definiu-o no artigo 5º, inciso XII, desta Lei como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".[58] Assim, pode-se afirmar que o consentimento pode ser considerado um processo de tomada de decisão do titular de dados, devendo ser-lhe garantida, segundo o artigo 2º, inciso II, da mesma Lei, autodeterminação informativa[59] suficiente para que sua manifestação de vontade seja de fato **livre, informada e inequívoca.**

Todavia, será elucidado a seguir que a atual conformação socioeconômica, denominada neste trabalho de **capitalismo de vigilância datificado** – em decorrência da relevância dos dados para a estruturação da arquitetura de vigilância unilateral descrita por Zuboff e Pasquale –, proporciona um **tolhimento à liberdade de escolha** dos titulares de dados, a partir de técnicas manipulatórias comportamentais. A partir da análise dos campos da Psicologia e da Economia Comportamental, será analisado em que medida a tomada de decisão dos consumidores pode ser considerada livre diante dos riscos de manipulação e persuasão que serão apresentados.

Apesar de o livre fluxo informacional promover uma maior circulação de informação, tal cenário não necessariamente significa que os consumidores tomam melhores decisões no panóptico digital. Isso porque temos de diferir até que ponto a informação deixa de ser **informativa** e passa a der **deformadora**; bem como em que medida a comunicação não é mais **comunicativa**, mas sim meramente **cumulativa**.[60]

---

[57] SUNDMAEKER, Harald et al. Vision and challenges for realizing the Internet of Things. *Cluster of European Research Projects in the Internet of Things*, European Commission, v. 3, n. 3, 2010, pp. 34-36.

[58] BRASIL, Lei nº 13.709, de 14 ago. 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, Acesso em 15 nov. 2022.

[59] O conceito de autodeterminação informativa será melhor elucidado na seção II deste trabalho, porém cabe pontuar, neste momento, que se relaciona com o poder que o titular tem sobre seus próprios dados.

[60] Ideia extraída de: HAN. *Op. cit.*, 2018, p. 106.

A vigilância ostensiva e a punição normalizadora de Foucault ganham, assim, uma roupagem de **vigília incógnita e sanção autoexploratória**, ambas socialmente aceitas por dois principais motivos: i) o desconhecimento por parte dos titulares dos riscos advindos do poder econômico que poucos agente têm do processamento de seus dados e ii) a manipulação sofrida pelos titulares, que, sabendo ou não desses processos persuasivos, não conseguem encontrar outra solução a não ser se submeterem a práticas sub-reptícias de empresas para a extração de seus dados.

Antes de versar sobre as práticas manipulatórias, contudo, perpassaremos um ponto relevante para sua compreensão: o advento das plataformas digitais e *big techs* na economia de dados, as quais reconfiguraram as relações econômicas e as próprias noções de como seus consumidores priorizam o tratamento de seus dados pessoais. A partir disso, verificaremos os principais agentes econômicos responsáveis pela extração ilícita de dados pessoais no ambiente digitalizado, os quais propulsionam e retroalimentam o capitalismo de vigilância datificado.

CAPÍTULO 2 – Entidades privadas vigilantes: os principais atores responsáveis pela extração de dados pessoais e pelo seu consequente *feedback looping* (positivo e negativo)

Apesar de seu protagonismo no ambiente digitalizado, as plataformas digitais e *big techs*, como veremos adiante, não são as únicas entidades privadas cuja operacionalização e arquitetura econômica viabilizam a extração massiva sub-reptícia de dados pessoais de usuários e consumidores no contexto vigilante datificado. Nesse sentido, para que possamos constatar quais são os principais agentes econômicos que manipulam titulares com fins de obterem seus dados pessoais, torna-se importante, antes de mais nada, compreendermos como se dá o protagonismo das empresas de tecnologia neste cenário, bem como quais são os impactos gerados por sua atuação na economia e, por conseguinte, nos seus usuários e consumidores.

2.1 - Plataformas digitais e *big techs*: definições, esferas de poder e assimetria informacional

Uber, iFood, Apple, Microsoft, Alphabet, Meta, Amazon… esses são alguns dos nomes de plataformas e *big techs* mais conhecidas e utilizadas pela população ocidental atualmente. Para que passemos à análise de seu papel no capitalismo de vigilância datificado, bem como suas repercussões na modulação comportamental de seus usuários e consumidores, cabe ressaltar primeiramente as diferenças conceituais e operacionais entre elas.

Plataformas digitais, segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), são "serviços digitais que facilitam a interação entre dois ou mais [...] usuários que interagem [...] via internet"[61]. Uma plataforma permite interações diretas entre dois ou mais grupos em que cada um é filiado à plataforma de algum modo, normalmente através de investimentos específicos,[62] seja oferecendo dados pessoais ou anúncios publicitários, por exemplo.

[61] Tradução livre: "Therefore, the definition used in this report is that an online platform is a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet." - OCDE. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. OECD Publishing, Paris, 2019, p. 20-23. Disponível em: <https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en#page22>. Acesso em: 15 de nov. 2022.

[62] HAGLU, Andrei; WRIGHT, Julian. Multi-Sided Platforms, *International Journal of Industrial Organization*, vol. 43, issue C, 2015, pp. 162-163.

Ademais, a existência das plataformas pressupõe a dependência de ambos os lados de grupos de clientes que queiram interagir mediante seus serviços e produtos, mas que não conseguem captar o valor de sua atração mútua por si mesmos; bem como necessita da confiança destes para a facilitação de interações de criação de valor entre eles.[63]

Por sua vez, *big techs* são as maiores empresas de tecnologia que possuem a dominância de mercado[64] do seu setor. Usualmente, são resumidas, porém não limitadas, pela sigla GAFAM: Google – remetendo à subsidiária do grupo Alphabet –, Amazon, Facebook – referindo-se ao grupo Meta –, Apple e Microsoft. Essas empresas têm sido requisitadas pelos consumidores pela sua habilidade de atendimento aos seus interesses e preferências, além de seu poder de influenciar a dinâmica competitiva em mercados de múltiplos lados, sendo muitas vezes monopólios por natureza.[65]

Seus modelos de negócio são baseados em "interações diretas de seus usuários e de seus dados, gerados como subproduto essencial dessas interações".[66] Uma característica que distingue as *big techs* das demais empresas é a sua capacidade de ultrapassar limites à escala de produção ao utilizar os dados de seus usuários e aproveitar os "efeitos de rede inerentes aos serviços digitais".[67] Os efeitos de rede, neste caso considerados como externalidades diretas positivas, podem ser definidos como resultados de um benefício que o consumidor usufrui a partir do uso de um bem, o que muitas vezes depende do número de outros consumidores que compram bens compatíveis.[68]

---

[63] EVANS, Davis S.; SCHMALENSEE, Richard. *The Antitrust Analysis of Multi-Sided Platform Business*, Cambridge, NBER Working Paper n. 18783, 2013.

[64] Vale ressaltar neste ponto que, para o Direito Concorrencial, a dominância de mercado tem intrínseca relação com a definição de mercado relevante, que, no contexto da *data-driven economy*, torna-se fluida em razão da própria fluidez da substituibilidade de produtos e serviços do mundo digital. "Em muitos casos, além das eventuais zonas de sobreposição, há fundadas dúvidas sobre que produtos ou serviços, apesar de não idênticos, são funcionalmente semelhantes, a ponto de integrarem o mesmo mercado relevante." – FRAZÃO, Ana. Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência. In: *Empresa, Mercado e Tecnologia*, 2019, p. 547.

[65] Ideia extraída de: MARCIANO, Alain et al. Big data and big techs: understanding the value of information in platform capitalism, *European Journal of Law and Economics*, Springer, n. 50, pp. 345–358, 2020, p. 354.

[66] Tradução livre: "Their business model revolves around the direct interactions of users and the data generated as an essential by-product of these interactions" – CARSTENS, Agustín et al. Regulating big techs in finance, BIS Bulletin, n. 45, 2021, p. 3.

[67] Tradução livre: "The distinguishing feature of big techs is that they can overcome limits to scale by utilising user data from their existing businesses to scale up rapidly by harnessing the inherent network effects in digital services. – *Ibid*., p. 3.

[68] KATZ, Michael; SHAPIRO, Carl. Network externalities, competition and compatibility. The American economic review, v. 75, n. 3, pp. 424-440, 1985.

Por exemplo, quanto mais usuários de uma determinada *big tech* a utilizá-la, mais tornar-se-á atraente, menos custosa e mais valiosa sob os olhos de um novo usuário entrante. Ademais, a entrada de um novo usuário na *big tech* gera um ganho específico para este usuário e um ganho social para o conjunto de usuários de toda a empresa. Há, portanto, uma dinâmica de retroalimentação que fomenta o sistema de lucro empresarial, tanto de *big techs*, quanto de plataformas digitais em ***feedback looping* positivo** – pois estas também se beneficiam dos efeitos de rede dos serviços digitais.

Ainda mais ao considerarmos que o *Big Data* passou a permitir às plataformas e *big techs* a expansão de sua atuação por meio da mineração, utilização e análise dos dados de seus usuários, essas empresas adquiriram tamanha proporção no capitalismo de vigilância datificado, que, vale rememorar, muitas delas possuem hoje posição dominante em diversos mercados, tornando-se inclusive o próprio mercado.[69] Surge daí o receio do uso desse poderio para proteger e fomentar ainda mais seu domínio, mesmo **em detrimento dos titulares de dados**.

A geração de valor por meio da extração dos dados pessoais, bem como os impactos sobre seus titulares, pelas grandes plataformas e *big techs* somente é possível em decorrência de sua atuação nas diversas **esferas de poder de influência** de mercado. A primeira esfera está representada no **poder de conexão** (*gatekeeper power)*,[70] visto que as plataformas digitais põem em contato diversos agentes econômicos, consumidores e até mesmo governos, sendo muitas vezes a única opção de interação e intermédio possível entre esses atores da economia.

Outra importante dimensão é o **poder de alavancagem** (*leveraging power*),[71] uma vez que essas empresas passam a integrar os mesmos mercados de vários de seus usuários e, desse modo, fazem com que haja a possibilidade de que as plataformas digitais passem a privilegiar seus próprios interesses em detrimento daqueles dos seus consumidores. Ademais, as plataformas e *big techs* detêm também o **poder de extração e exploração de dados pessoais[72]**, já que podem monitorar seus usuários facilmente e associar um grande número de informações úteis sobre eles, obtendo, assim, diversas vantagens econômicas.

---

[69] THE ECONOMIST. *The new titans.* And how to tame them. 20 jan. 2018. Disponível em: <https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans>. Acesso em: 15 nov. 2022.
[70] FRAZÃO, *Op. cit*., 2019, p. 540.
[71] Idem.
[72] Idem.

Uma outra extensão importante a ser destacada é a do **poder de comunicação**[73], a partir do momento em que se parte da premissa de Herbert Simon de que a riqueza de informação gera uma pobreza de atenção.[74]-[75] Dessa maneira, as plataformas digitais e *big techs* podem filtrar as informações e direcioná-las a seus usuários, moldando-as de acordo com o interesse de cada um deles, configurando a dimensão do chamado **poder de influência e de manipulação**.[76]

Essas esferas de poder demonstram um acúmulo de poder econômico maciço por parte dessas empresas, de modo a muitas vezes ameaçar a autodeterminação informativa de seus usuários, bem como sua privacidade e o próprio direito à proteção de seus dados pessoais, que serão abordados adiante, especificamente na seção II deste trabalho.

Dentre as formas de dominação praticadas por essas empresas, vale frisar a **dominação informacional** que detêm sobre seus usuários e consumidores, a partir do momento que tratam seus dados sob um monopólio digital e direcionam-lhes anúncios de produtos e serviços personalizados – justamente através do processamento das informações dos dados que foram-lhe fornecidos. Não é incomum que plataformas digitais e *big techs* se utilizem de técnicas de ***profiling***[77] **e** ***microtargeting***[78] – isto é, perfilização[79] comportamental dos seus usuários e anúncios direcionados de acordo com as preferências particulares de cada um deles,

---

[73] *Idem.*

[74] SIMON, Herbert. Designing organizations for an information-rich world. In: GREENBERGER, M. *Computers, communications and the public interest*. Baltimore: The John Hopkins Press, 1917.

[75] Tal premissa coaduna-se com aquela trazida por Byung-Chul Han em *No enxame: perspectivas do digital*, no capítulo Cansaço da Informação, em que o autor sugere que a quantidade de informações não gera necessariamente tomadas de decisões otimizadas. Vide: HAN, Byung-Chul. No enxame: perspectivas do digital, Petrópolis, RJ: Vozes, 2018, pp. 103-108.

[76] FRAZÃO, *Op. cit*., 2019, p. 540.

[77] *Profiling* pode ser definido como "uma técnica em que um conjunto de características de uma determinada classe de pessoa é inferido a partir de experiências passadas e, em seguida, dados armazenados são pesquisados para indivíduos com um ajuste quase perfeito a esse conjunto de características" - CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law & Information Science*, v. 4, p. 403, 1993.

[78] *Microtargeting* é uma tecnologia que "consiste em classificar indivíduos a partir de seus interesses, gostos, idade, localização geográfica, classe social, entre outras características, a partir dos dados pessoais obtidos online, para então expô-los à informações com potencial de convencê-los a alguma prática, seja o consumo de algum produto ou serviço, ou ainda utilizando para conquistar o apoio e voto em eleições, inclusive presidenciais - NEVES, João Marcos Santos das. *Proteção de dados na internet a partir do estudo de caso Cambridge Analytica*: parâmetros para um debate internacional, Trabalho de Conclusão de Curso, Universidade Federal Fluminense, Macaé, 2020, p. 18.

[79] A nomenclatura perfilização para se referir às técnicas de profiling é usada por alguns pesquisadores brasileiros, dentre eles: KANASHIRO, Marta M. Apresentação*: Vigiar e resistir*: a constituição de práticas e saberes em torno da informação. Ciência e Cultura, v. 68, n. 1, p. 20-24, 2016. DOS REIS PERON, Alcides Eduardo; ALVAREZ, Marcos César; CAMPELLO, Ricardo Urquizas. Apresentação do Dossiê: *Vigilância, Controle e Novas tecnologias*. Mediações-Revista de Ciências Sociais, v. 23, n. 1, 2017, p. 11-31.

respectivamente – para otimizar a operacionalização de seus serviços e aumentar o engajamento dos consumidores à sua dinâmica de produção.

Todavia, o uso da tecnologia para modulação comportamental não é restrito às plataformas digitais e *big techs*, sendo amplamente utilizadas por companhias de outros setores da economia, por birôs de crédito – por exemplo, para classificar consumidores e potenciais grupos de risco de devedores – e por *websites* de empresas de variados ramos econômicos. Passemos à sua análise.

2.2 – Demais atores econômicos do mundo digitalizado: empresas varejistas, birôs de créditos e *websites* de companhias de outros ramos econômicos

Em relação ao primeiro caso, diversas companhias do setor varejista fazem ou já fizeram uso de tecnologias de *marketing* direcionado e de reconhecimento facial a fim de obter dados pessoais de consumidores, por meio de práticas sub-reptícias, sob a justificativa de otimização de seus serviços. Porém, ao analisarmos as situações com maior clareza, notaremos que foram realizadas manipulações comportamentais aos consumidores, os quais tiveram diversos de seus direitos relativos ao âmbito do direito à proteção de dados e consumerista violados pelas empresas.

Um exemplo concreto do uso indevido de *marketing* direcionado foi o que fez a empresa **Target** em 2012, que, ao realizar modelagem e análise de dados de suas consumidoras para inferir sua possibilidade de gravidez e promover ações de *marketing* direcionado, antes mesmo que elas próprias contassem a seus familiares próximos. Ao coletar cerca de 25 dados relacionados a produtos atribuídos a uma pontuação de "previsão de gravidez"[80] associada a cada consumidora, a companhia foi capaz de prever não apenas a condição de gestação, como também estágios muito específicos de gravidez das clientes. Assim, a Target iniciou o envio de cupons para itens de maternidade às residências dessas clientes de acordo com suas "pontuações" de gravidez. Tal situação repercutiu em descobertas antecipadas e indesejadas sobre as condições dessas consumidoras, o que constitui uma clara violação a seus direitos, tanto no âmbito consumerista, quanto no campo de proteção de dados pessoais.

[80] *Cf.*: *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4ccdae5b6668>. Acesso em 12 dez. 2022.

Por outro lado, em relação ao emprego de tecnologias de reconhecimento facial para a extração de dados pessoais, importa destacar o caso da varejista **Hering** que, utilizando-se de inteligência artificial em sua loja no Shopping Morumbi, em São Paulo, conseguiu captar as reações dos consumidores e traçar seus perfis de consumo – *profiling* –, sem informação prévia clara e adequada, bem como sem o devido consentimento de seus clientes. Apesar de o reconhecimento facial já não ser mais utilizado, a Senacon (Secretaria Nacional do Consumidor) apurou diversas violações ocorridas à época dos fatos, no início de 2019. Além de constatar que a empresa se aproveitou da vulnerabilidade do consumidor, também foi averiguada pela Senacon a violação do direito à informação e aos direitos de personalidade dos cidadãos, visto que as imagens foram utilizadas para fins comerciais sem consentimento prévio. Todas essas práticas levaram à condenação da Hering ao pagamento de uma multa de R$ 58.767,00, destinada ao Fundo de Defesa de Direitos Difusos (FDDD).[81]

No que tange aos birôs de crédito, ao utilizarem técnicas de *profiling*, em um sistema de perfilização enviesado, podem fazer com que uma pessoa que more em determinado bairro ou local periférico e que tenha certas características – seja de gênero, idade, raça ou nível de ensino – seja discriminada em uma seleção de emprego ou classificada como potencial inadimplente ao tentar conseguir um empréstimo bancário. Segundo Zanatta,

> Essas pessoas não sabem que estão sendo discriminadas e que o potencial empregador leva em consideração seu *credit scoring* (sistema de pontuação de crédito) e o "grau de risco" determinado de forma matemática, alocando a pessoa dentro de um "grupo social" estatisticamente modelado. Um dos pontos cruciais da perfilização é que ela está mais relacionada a grupos sociais do que ao indivíduo em si, o que provoca uma tensão ainda não resolvida na matriz individualista da proteção de dados pessoais. [82]

A classificação de pessoas pertencentes a certo grupo de risco foi relatada por Cathy O'Neil, em *Weapons of math destruction,*[83] para descrever as consequências que sistemas de *profiling* podem ocasionar aos titulares de dados. A autora relata, por exemplo, a influência de vieses na elaboração de fórmulas matemáticas utilizadas pelos birôs de créditos estadunidenses Equifax e Experian, "que pontuam a população em uma escala de 0 a 1000 utilizando milhares

---

[81] *Cf.*: *Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial:* Secretaria Nacional do Consumidor condenou a empresa ao pagamento de multa de R$ 58,7 mil por violações ao CDC. Disponível em: <https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial>. Acesso em 12 dez. 2022.

[82] ZANATTA, Rafael A. F. *Perfilização, Discriminação e Direitos*: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, 2019, p. 2. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 16 de nov. de 2022.

[83] O'NEIL, Cathy. *Weapons of math destruction*: How big data increases inequality and threatens democracy. Broadway Books, 2016.

de pontos de dados e metodologias obscuras para determinar como uma pessoa se enquadra em um certo 'grupo social' com características semelhantes a ela".[84]

A obscuridade algorítmica, também denominada opacidade dos algoritmos,[85] aumenta a assimetria da informação e, por conseguinte, a dominação informacional característica do capitalismo de vigilância datificado - no qual os processadores de dados tudo sabem dos titulares, enquanto estes nada sabem daqueles. Isso repercute no que Virginia Eubanks descreve como um ***feedback looping* de injustiça**[86], em decorrência da viabilidade da coleta de dados e monitoramento de grupos socialmente vulnerabilizados.

Eubanks elucida que "a maioria das pessoas são escolhidas para escrutínio digital como membros de grupos sociais, não como indivíduos".[87] Os dados extraídos desses grupos servem para incrementar a marginalidade, quando tais coletividades são alvo de "algoritmos preditivos, análises de risco e sistemas automáticos de elegibilidade".[88]

A algoritmização para finalidades discriminatórias não se resume, todavia, aos birôs de crédito. Veremos adiante, especificamente no subcapítulo 3.1, que diversos *websites* – dos mais diversos setores da economia e da sociedade, a exemplo de companhias aéreas, empresas de cosméticos, entidades privadas de organização de eventos e veículos de comunicação da imprensa – se utilizam de técnicas que incrementam a assimetria informacional entre fornecedores e consumidores – a partir do emprego de mecanismos que tolhem a capacidade decisória do titular-consumidor –, bem como fomentam determinados comportamentos a partir da análise e predição de perfis de consumo – o que repercute em uma discriminação socioeconômica de titulares de dados.

Portanto, percebe-se que, enquanto as plataformas, *big techs* e demais companhias do contexto datificado se beneficiam da digitalização por meio de um *feedback looping* positivo, os titulares sofrem consequências também em *feedback looping*, porém negativo. Muitas das externalidades positivas advindas dos efeitos de rede dessas empresas têm como consequência a discriminação massiva de seus usuários e consumidores, ainda mais ao considerarmos as

[84] ZANATTA, *Op. c*it. 2019, p 2.
[85] Essa nomenclatura remete ao debate inaugurado por Frank Pasquale sobre o *one-way mirror* e as caixas pretas dos algoritmos - PASQUALE. *Op. cit.*, 2015
[86] ZANATTA, *Op. cit.*, 2019, p. 3.
[87] EUBANKS, Virginia. *Automating inequality*: How high-tech tools profile, police, and punish the poor. St. Martin's Press, 2018, p. 6.
[88] ZANATTA, *Op. cit.*, 2019, p. 3.

técnicas manipulatórias utilizadas pelos processadores de dados para a extração de seus dados pessoais.

Tais práticas serão elucidadas no próximo capítulo a partir de três principais abordagens que melhor sistematizam a persuasão e manipulação de titulares de dados no capitalismo de vigilância datificado, sendo elas: a Economia Comportamental, a Economia Psíquica dos Algoritmos e a Neurociência.

CAPÍTULO 3 – Técnicas manipulatórias utilizadas contra titulares de dados

Antes de mais nada, para que possamos compreender como se dá a aplicação das práticas de cunho manipulatório contra consumidores, enquanto consumidores e titulares de dados de entidades privadas inseridas no ambiente digitalizado, torna-se importante estabelecer o conceito de manipulação adotado neste trabalho.

A conceituação de manipulação que será o fio condutor de todo este capítulo tem como alicerce o que Susser, Roessler e Nissenbaum definem como "[...] uma espécie de influência – uma tentativa de mudar a forma como alguém se comportaria sem as intervenções do manipulador".[89] Seguimos ainda seu entendimento, elucidado no artigo *Online Manipulation,* de que a manipulação esconde uma faceta oculta de influenciar uma subversão dos poderes decisórios dos sujeitos.[90]

Diante disso, primeiramente optamos por descrever como o campo da *Behavioral Economics* pode auxiliar na compreensão do contexto manipulatório do comportamento de titulares de dados e consumidores na economia digital para, de maneira gradativa – de acordo com níveis de intrusão nos aspectos decisórios e na *psique* dos indivíduos –, enfim aprofundarmo-nos na Economia Psíquica dos Algoritmos e na Neurociência.

3.1 – A Economia Comportamental: *(hiper)nudges, dark patterns* e dissonância cognitiva

A Economia Comportamental, também denominada *Behavioral Economics*, é "o estudo das influências cognitivas, sociais e emocionais observadas sobre o comportamento econômico das pessoas"[91], aproximando-se tanto da Psicologia Comportamental, quanto da Cognitiva, ao analisar previsões comportamentais a partir da inferência de estímulos emocionais e cognitivos. Ademais, essa ciência se utiliza principalmente do método empírico da experimentação para desenvolver teorias relativas à tomada de decisão pelo ser humano.

---

[89] Tradução livre. "Manipulation (...) is a kind of influence - an attempt to change the way someone would behave absent the manipulator's interventions." In: SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. *Online Manipulation:* Hidden Influences in a Digital World, 4 Geo. L. Tech. Rev. 1, 2019, p. 13.

[90] *Ibid*., p. 3.

[91] SAMSOM, Alain. Introdução à economia comportamental: a economia comportamental e experimental. *In:* AVILA, Flávia; BIANCHI, Ana Maria. (org.). *Guia de Economia Comportamental e Experimental*, 2ª ed., São Paulo: InBehavior Lab, pp. 26-60, 2019, p. 26.

Logo, é o campo da ciência econômica que combina elementos da Psicologia Behaviorista[92] para entender como e por que as pessoas se comportam e agem de determinada forma. Distingue-se da Economia Neoclássica por assumir que a maioria das pessoas tem preferências definidas e tomam decisões bem informadas e interessadas em si mesmas com base em predileções prévias.[93]

Baseando-se em grande parte no trabalho de Richard Thaler, da Universidade de Chicago, a Economia Comportamental examina as diferenças entre o que as pessoas deveriam fazer e o que elas realmente fazem, bem como as consequências dessas ações. Nesse sentido, demonstram que os agentes nem sempre tomam o que os economistas neoclássicos consideram a decisão "racional" ou "ótima", mesmo que tenham as informações e as ferramentas disponíveis para fazê-la, a partir do momento em que comprova que a disposição para correr riscos é influenciada pelo modo que as escolhas são apresentadas.

Outros grandes nomes do campo da *Behavioral Economics* que merecem destaque são Amos Tversky e Daniel Kahneman, ambos psicólogos israelenses que, nos anos 1970 e 1980, identificaram várias desconfianças consistentes na forma com que as pessoas faziam julgamentos, constatando que muitas vezes os indivíduos confiam em informações facilmente lembradas, em vez de acreditar em dados reais, ao avaliar a probabilidade de um determinado resultado, um conceito conhecido como o "heurístico de disponibilidade".[94]

Daniel Kahneman, em seu clássico *Rápido e Devagar,* expõe que tirar conclusões precipitadas é eficaz – em um sentido de afirmação de convencimento pessoal – se há grandes probabilidades de que as conclusões estejam corretas, e se o custo ocasional de um possível erro for "aceitável", bem como se "o 'pulo' poupa grande tempo e esforço".[95] Contudo, o psicólogo alerta que pular para conclusões é arriscado quando a situação é pouco familiar, pois existem muitos fatores em jogo e não há o devido tempo para reunir a quantidade necessária de

---

[92] A Psicologia Behaviorista ou Psicologia Comportamental é o campo das ciências naturais fundado por John B. Watson que analisa "a previsão e o controle do comportamento humano". – WATSON, John B. A psicologia como o behaviorista a vê, *Temas em Psicologia,* vol. 16, n. 2, pp. 289-301, 2008, p. 298.

[93] WITYNSKI, Max. *Behavioral economics, explained,* 2020. Disponível em: <https://news.uchicago.edu/explainer/what-is-behavioral-economics#:~:text=Behavioral%20economics%20combines%20elements%20of,decisions%20based%20on%20those%20preferences.>. Acesso em 20 nov. 2022.

[94] *Idem.*

[95] KAHNEMAN, Daniel. *Rápido e Devagar.* Duas formas de pensar. Tradução de Cassio Leite, São Paulo: Objetiva, 2011, p. 60.

informação.[96] Segundo afirma o autor, essas são as situações em que erros intuitivos são configuráveis.[97]

Ainda, no que tange a decisões precipitadas, cuja relevância é considerada pela Economia Comportamental, Richard Thaler e Cass Sunstein cunharam o termo *nudge*[98] para definir "uma maneira de manipular as escolhas das pessoas para levá-las a tomar decisões específicas",[99] sem propriamente coagi-las a tomar essa decisão, mas sim influenciá-las. Nos termos dos próprios autores,

> Um nudge [...] é qualquer aspecto da arquitetura de escolha que **altera o comportamento das pessoas de um modo previsível sem proibir quaisquer opções nem alterar significativamente seus incentivos econômicos.** Para que uma intervenção seja considerada um mero nudge, deve ser fácil e barato evitá-la. Nudges não são imposições. Dispor as frutas ao nível do olhar é considerado nudge. Proibir junk food, não.[100] (grifos nossos)

Ademais, cabe pontuar que o termo *nudge* advém da língua inglesa e pode ser traduzido como pequeno empurrão ou cotovelada. Para Thaler e Sunstein, o *nudge* pode ser considerado como um mecanismo de controle comportamental, uma iniciativa que direcionaria as pessoas para determinados caminhos, todavia, em concomitância apontaria a direção de decisão para o indivíduo, isto é, permitiria que eles possuíssem certa liberdade para segui-lo da forma como bem desejassem. Desse modo, esse incentivo não pode se dar de forma imperativa, uma vez que o *nudge*, pelo menos a princípio, se pauta por uma suposta liberdade do sujeito. Por isso,

> [...] o motivo de caracterizar o *nudge* como um mecanismo de economia comportamental, tendo em vista que está voltado para lidar com o comportamento humano. Esta é uma das razões que atrai as instituições públicas e privadas para atingir seus objetivos específicos. Além disso, os custos para a sua implementação podem ser baixos e a taxa de efetividade é considerada alta. Esses elementos fazem do *nudge* um grande atrativo.
> Dentre as formas de *nudges*, possuímos o GPS, aplicativos que calculam a quantidade de calorias que foram ingeridas pela pessoa no dia anterior, mensagens de texto que

[96] Hoje há divergências quanto à quantidade de informação ser sinônimo de melhor tomada de decisão. Byung-Chul Han, em *No Enxame: Perspectivas do do digital* (2018), explana que mais informação e comunicação não esclarecem o mundo por si mesmo, logo a transparência não seria sinônimo de clarividência. Deve-se, ademais, diferir até que ponto a informação deixa de ser informativa e passa a ser deformadora; e até que ponto a comunicação não é mais comunicativa, e sim cumulativa. – HAN. *Op. cit*., 2018, p. 106.

[97] KAHNEMAN, *Op.cit.*, 2011.

[98] SUNSTEIN, Cass R.; THALER, Richard H. *Nudge:* Improving Decisions About Health, Wealth, and Happiness. New Haven: Yale University Press, 2008.

[99] WITYSNKI, *Op. cit*., 2020.

[100] SUNSTEIN; THALER. *Op. cit*., 2008, p. 6.

> informam o vencimento de uma conta ou que informam o agendamento de uma consulta, o cadastro em planos de pensão, dentre outros.[101]

Pautando-se nas premissas de Thaler e Sunstein, a professora Karen Yeung, da Universidade de Birmingham, identificou que o *Big Data* possibilita ainda a prática de *hipernudges,*[102] que seriam *nudges* potencializados pela sofisticação do processamento algorítmico, o que oferece percepções preditivas exatas relativas a hábitos, preferências e interesses de consumidores.[103] Com isso, há uma "canalização das escolhas dos usuários"[104] de plataformas e *big techs* pela arquitetura do algoritmo utilizado pelos *hipernudges*, de maneira a enviesar seu processo decisório sutil e eficientemente, repercutindo em consequências positivas e negativas para os indivíduos.

Logo, apesar de haver um viés evidentemente manipulativo do *nudge,* há o usufruto de benefícios por parte dos indivíduos enquanto sujeitos manipulados, principalmente quando há a existência de três fatores envolvidos no processo de tomada de decisão: experiência, boas informações e *feedback* rápido.[105] Um bom exemplo disso seria o apontado por Alain Samson, outro expoente da área do *Behavorial Economics*:

> Por exemplo, o impacto de fumar é mais perceptível no decorrer dos anos, enquanto o efeito desse hábito sobre as células e órgãos internos geralmente não se evidencia para o indivíduo. Tradicionalmente, o feedback genérico destinado a induzir uma mudança comportamental limita-se a informações como os custos econômicos do comportamento prejudicial à saúde e suas possíveis consequências ao organismo (Diclemente et al., 2001). Programas mais recentes voltados para a mudança de comportamento, como o que usa aplicativos de celular para ajudar o usuário a parar de fumar, hoje fornecem feedback comportamental positivo e personalizado, que pode incluir o número de cigarros não fumados e o dinheiro poupado, além de informações sobre melhora da saúde e prevenção de doença.[106]

Todavia, podemos averiguar também consequências negativas do emprego do *nudge,* notadamente quando avaliamos a prática das denominadas *dark patterns* no ambiente digital. *Dark patterns* é o conceito usado para definir as estratégias que "ou dificultam que os

---

[101] SOUZA, Luciana Cristina et al. *Análise crítica da orientação de cidadãos como método para otimizar decisões públicas por meio da técnica nudge*, *In*: Revista Brasileira de Políticas Públicas - Programa de Mestrado e Doutorado em Direito do UniCEUB. Vol. 8, n. 2 (ago. 2018). Brasília: UniCEUB, 2011, p. 238.

[102] YEUNG, Karen. *Hypernudge*: Big Data as a mode of regulation by design, Information, Communication and Society, v. 10, n.1, pp. 118-136, 2016.

[103] *Ibid*., p. 119.

[104] *Idem.*

[105] SUNSTEIN; THALER. *Op. cit*., 2008.

[106] SAMSOM. *Op. cit*., 2019, p. 30.

consumidores expressem suas reais preferências, ou que os manipulam para que tomem ações que não sejam compatíveis"[107] com seus objetivos originários.

Essas práticas guardam intrínseca relação com o *nudge,* visto pré-selecionarem escolhas, destacarem ou esconderem botões de opção para compra de produtos e/ou frustrar com frequência consumidores a fim de persuadi-los a tomar decisões "contra as suas preferências ou expectativas".[108] De acordo com relatório publicado pelo Stigler Center, por mais que a utilização de interfaces chamativas e até mesmo promoções auxiliem na venda de um produto considerado lícito, fazer isso usando técnicas manipulatórias em detrimento dos consumidores – aproveitando-se de sua vulnerabilidade –, pode constituir prática ilícita.[109]

É o que, corroborando com o disposto no referido relatório, afirma o Subcomitê estadunidense de Direito Antitruste, ao explicitamente entrelaçar ambos os conceitos de *dark patterns* e *nudge*:

> Esses nudges comportamentais - referidos como dark patterns - são normalmente utilizados em linha de rastreio e publicidade on-line para aumentar o poder de mercado de uma empresa e 'maximizar a capacidade de uma companhia para extrair receitas dos seus usuários'. E no e-commerce, Jamie Luguri e Lior Strahilevitz observam que as dark patterns 'estão a prejudicar os consumidores ao convencê-los a entregar dinheiro ou dados pessoais em negócios que não refletem as preferências reais dos consumidores e que podem não servir aos seus interesses. Parece haver uma falha substancial do mercado no que diz respeito às dark patterns - o que é bom para os lucros do comércio eletrônico é ruim para os consumidores'.[110]

---

[107] FRAZÃO, Ana. *A falácia da soberania do consumidor*. O aumento da vulnerabilidade do consumidor na economia digital. Publicado em: 08/12/2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-emercado/falacia-soberania-do-consumidor-08122021>. Acesso em 20 nov. 2022.

[108] Tradução livre: "Companies can pre-select choices, highlight or hide buttons, or constantly nag consumers in order to push them to make decisions against their preferences or expectations. While using interfaces or promotions that help sell a product is not illegal, doing so in an extremely manipulative way can be, as these companies are strongly manipulating vulnerable consumers into buying products and services (...) they ultimately do not want." – ZINGALES, L.; ROLNIK, G.; LANCIERI, F. M. Final Report, Stigler Committee on Digital Platforms, *Stigler Center for the Study of the Economy and the State*, 2019, p. 12.

[109] *Idem.*

[110] Tradução livre: "These behavioral nudges – referred to as dark patterns – are commonly used in online tracking and advertising markets to enhance a firm's market power and "maximize a company's ability to extract revenue from its users." And in e-commerce, Jamie Luguri and Lior Strahilevitz observe that dark patterns "are harming consumers by convincing them to surrender cash or personal data in deals that do not reflect consumers' actual preferences and may not serve their interests. There appears to be a substantial market failure where dark patterns are concerned – what is good for ecommerce profits is bad for consumers." NADLER, J.; CICILLINE, D. N. Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations, *Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary,* 2020, p. 53.

Nessa senda, a seguir, serão apresentadas algumas tipologias[111] de *dark patterns* usualmente utilizadas no cotidiano de consumidores-titulares inseridos na arquitetura econômica vigilante, de modo a ilustrar o viés persuasivo dessas práticas nos processos de tomada de decisões de titulares de dados.

1) ***Dark patterns* de obstrução ou *confirmshaming***[112] – o primeiro exemplo é a técnica de induzir o usuário ou consumidor a não confirmar uma atitude que antes seria certamente realizada pelo mesmo, por isso a sua denominação "confirmação vergonhosa". Geralmente é utilizada quando um titular de dados deseja retirar sua inscrição de algum site ou plataforma, e costuma vir acompanhada de uma série de produtos e serviços que serão perdidos caso o titular deseje de fato cancelar sua inscrição. Vejamos algumas situações:

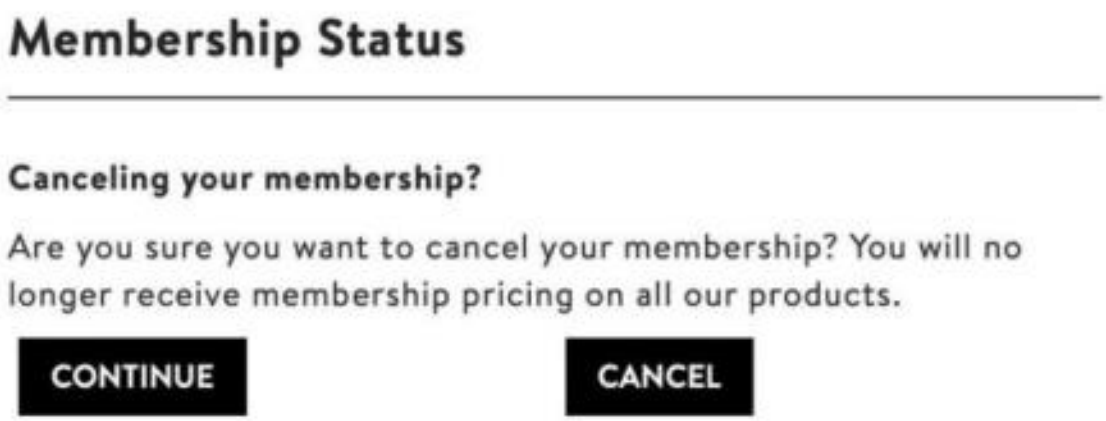


Figura 1: Situação real de cancelamento de inscrição em site. (Fonte: LUGURI, Jamie; STRAHILEVITZ, Jacob. Shining a light on dark patterns, *Oxford University Press*, The John M. Olin Center for Law, Economics and Business at Harvard Law School, 2021, p. 49)

[111] Os tipos apresentados neste capítulo não são taxativos, mas sim exemplificativos dentre as diversas facetas que as *dark patterns* podem se apresentar aos consumidores, enquanto usuários e titulares de dados.
[112] A nomenclatura é utilizada por: LUGURI, Jamie; STRAHILEVITZ, Jacob. Shining a light on dark patterns, *Oxford University Press*, The John M. Olin Center for Law, Economics and Business at Harvard Law School, 2021, p. 49.

Figura 2: Situação real de cancelamento de inscrição em site. (Fonte: edição da autora)[113]

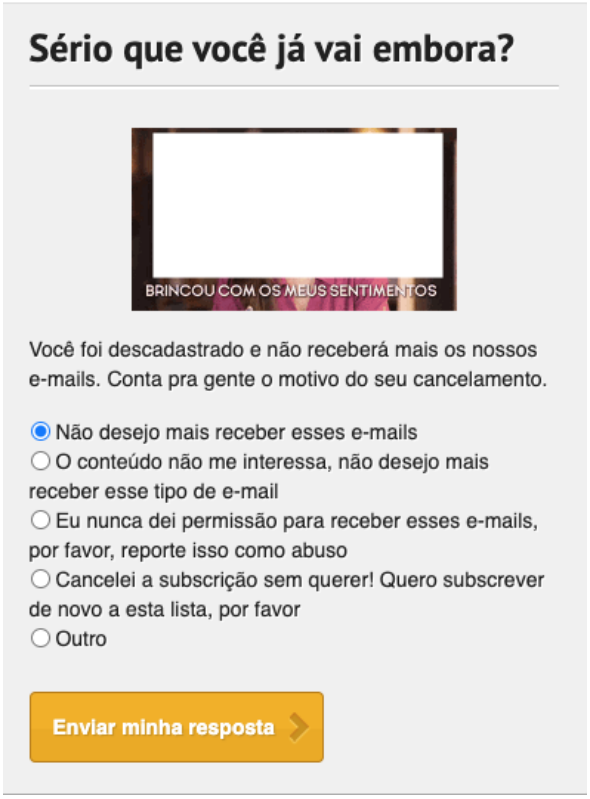


Figura 3: Situação real de cancelamento de inscrição em site. (Fonte: edição da autora)[114]

[113] Em experiência particular, já me deparei com obstáculos para cancelar uma inscrição por e-mail de ofertas de mestrado em uma universidade particular estadunidense. Diferentemente de outras situações, em que o cancelamento era automático, este direcionou-me para uma nova interface, requerendo a seleção de um *checkbox* a fim de confirmar minha decisão prévia. O link de acesso pode ser conferido em: < https://studio.mdl.io/REST/Handlers/unsubscribe.aspx?43297680;16296;20120713.3.Foxtrot.Account.a5cff51d_f41b_467c_8f02_4296dcd850c0;3be589c9_d6b1_409e_9413_815affdb303e;http%3a%2f%2fstudio.m.mdl.io%2funsubscribe>. Acesso em 20 nov. de 2022.

[114] A imagem da pessoa foi removida para não violar seus direitos à privacidade e à proteção de dados pessoais, já que não foi coletado seu consentimento válido para fins de divulgação neste trabalho. A arquitetura escolhida

2) ***Dark patterns* incômodas ou *nagging***[115]: ao se deparar com interfaces em seus *smartphones* ou computadores oferecendo-lhe duas únicas opções: aceitar (“*yes”*) ou rejeitar, talvez seguido de “por enquanto” ou talvez mais tarde (“*not now”*[116]), o envio de notificações de aplicativo ou site, o titular de dados vê-se diante das chamadas *nagging dark patterns*. O nome se dá pelo incômodo gerado pela intermitência que elas se apresentam ao consumidor, como se “vencessem-no” pela persistência e pelo cansaço. Confiramos alguns cenários:

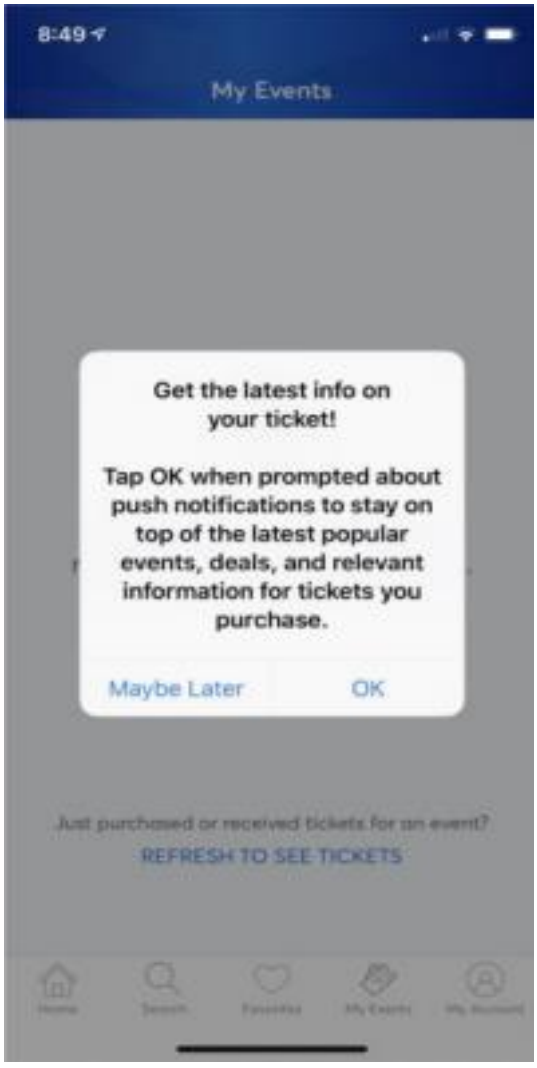


Figura 3: Situação real de *dark pattern nagging* em aplicativo (Fonte: LUGURI; STRAHILEVITZ. *Op. cit.*, 2021, p. 50)

pela *dark pattern* é claramente da tipologia *confirmshaming*, visto objetivar persuadir o consumidor a repensar sua atitude de cancelar sua inscrição. *Cf.:* <https://mepoupenaweb-mkt.activehosted.com/unsubscribe_result/1/11/3677a574171181dc4bff5ff34693acf8/0/1157/1265>.

[115] LUGURI; STRAHILEVITZ. *Op. cit.*, 2021, p. 50.

[116] O binômio é utilizado por: LUGURI; STRAHILEVITZ. *Op. cit.*, 2021, p. 49.

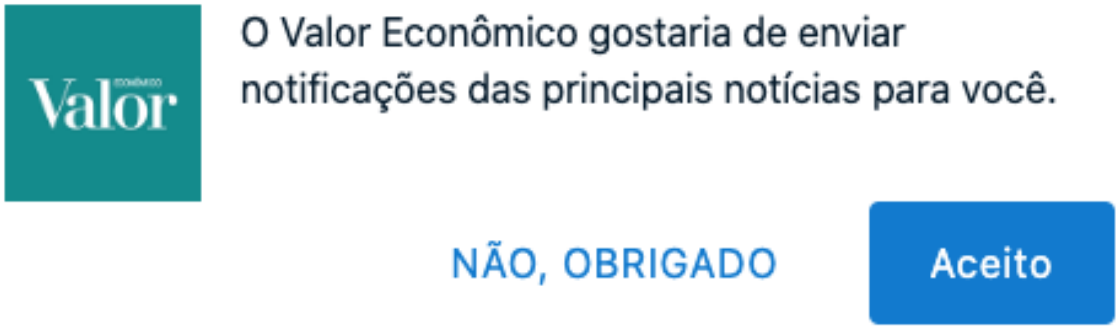


Figura 4: Situação real de *dark pattern nagging* em site (Fonte: edição da autora)[117]

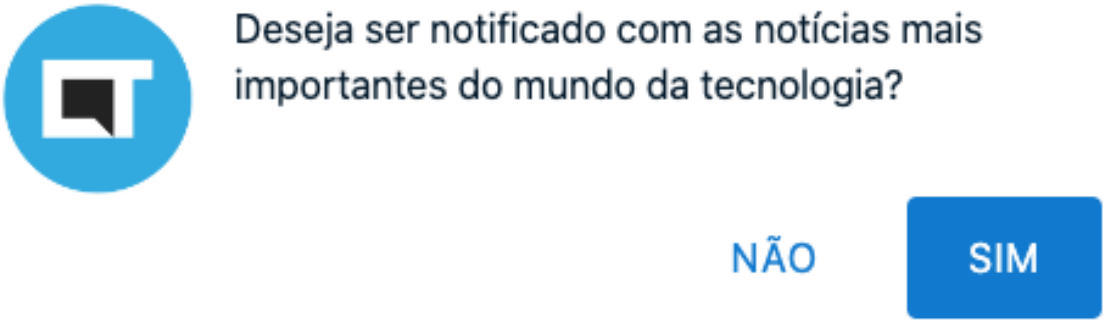
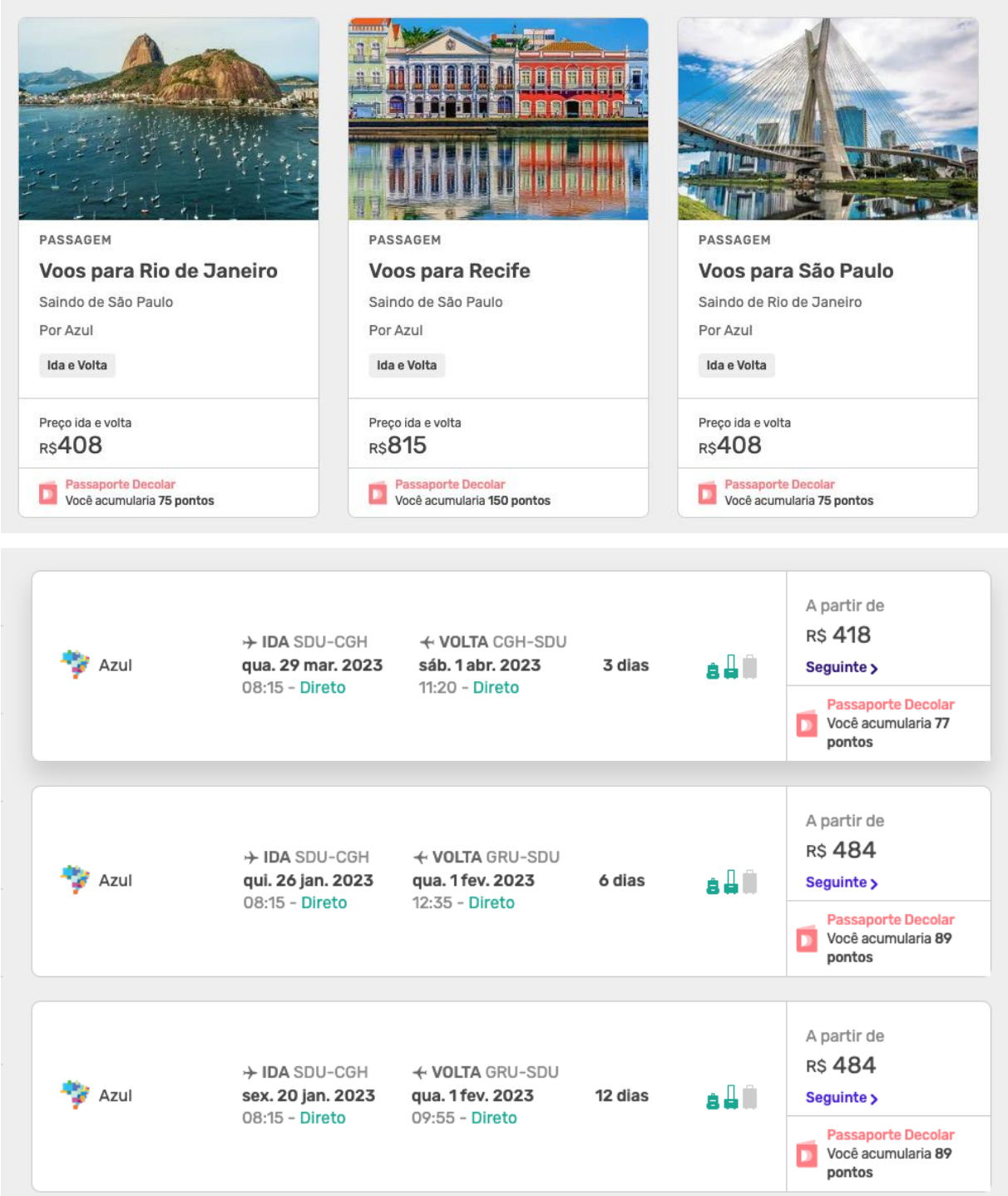


Figura 5: Situação real de *dark pattern nagging* em site (Fonte: edição da autora)[118]

3) ***Dark patterns* de isca e troca ou *bait and switch***: são aquelas cujo principal objetivo é atrair o consumidor a comprar um bem ou serviço anunciado em um site ou plataforma e, ao realizar a compra, este é surpreendido com uma oferta diferente da publicizada ou com uma barreira indesejada de anúncios[119] de produtos similares ou não. Vejamos:

[117] Todas as vezes que entro em diversos sites de notícias, incluindo o Valor Econômico, sou submetida a interfaces como esta para escolher se desejo receber notificações – já que nunca aceitei recebê-las. *Cf.*: <https://valor.globo.com/>. Acesso em 20 de nov. de 2022.
[118] Novamente, ao acessar um site ao qual recorro intermitentemente sobre novas tecnologias, deparei-me com a opção binária "sim" e "não". *Cf.*: < https://canaltech.com.br/>. Acesso em: 20 nov 2022.
[119] LUGURI; STRAHILEVITZ. *Op. cit.*, 2021, p. 50.



Figuras 6 e 7: Uma *dark pattern bait and switch* usualmente utilizada por companhias aéreas é bem exemplificada por estas duas imagens. O anúncio dos voos para São Paulo chama a atenção dos consumidores ao serem ofertados pelo preço de 408 reais. Todavia, ao clicarmos nas opções de voo, a sua maioria disponível é acima do preço de oferta. Outra característica abusiva deste anúncio publicitário importante de ser ressaltada é

que ele não informa o consumidor que não estão incluídas as taxas de serviço no preço anunciado, o que aumentará consideravelmente o preço final da passagem. (Fonte: edição da autora)[120]

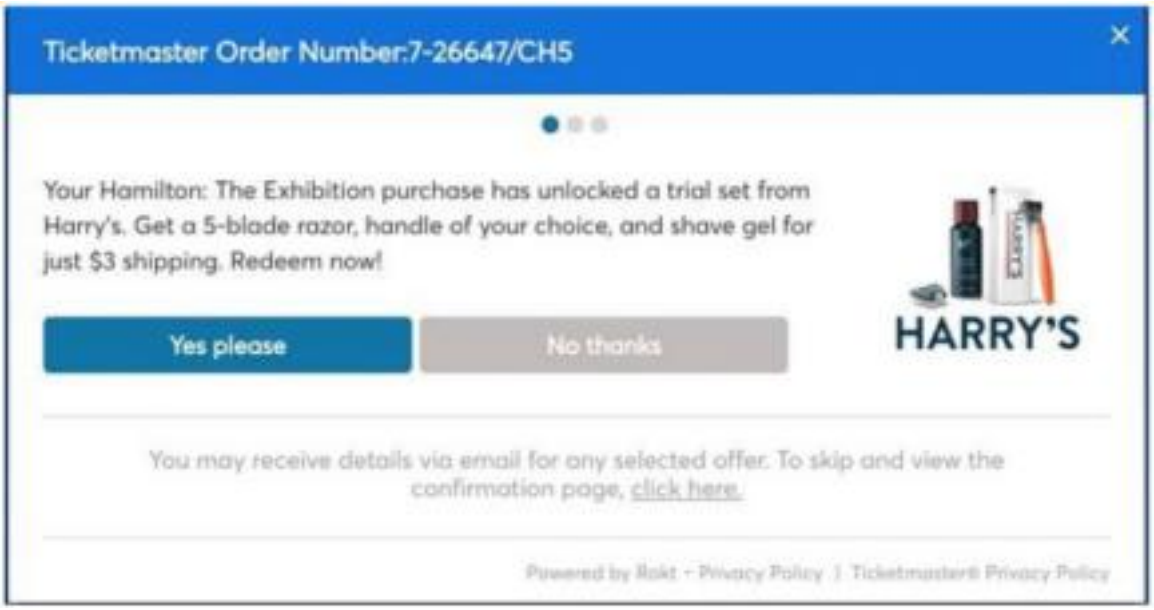


Figura 8: Situação real de *dark pattern bait and switch* em site (Fonte: LUGURI; STRAHILEVITZ. *Op. cit.*, 2021, p. 51)

4) ***Dark patterns* de evasão ou *sneaking***: o último exemplo a ser trazido constitui a prática da "tentativa de esconder, disfarçar ou atrasar a divulgação de informação relevante para o usuário ou consumidor".[121] Geralmente essas *dark patterns* são usadas em termos de uso e políticas de privacidade de plataformas e de *cookies*[122] de navegação de sites, seja pela utilização de interfaces novas passíveis de fácil demérito pelo titular de dados ou pela utilização de linguagem inacessível – com termos técnicos, de difícil compreensão para aqueles que não têm expertise na área da tecnologia. Seguem algumas situações ilustrativas e uma situação concreta:

[120] *Cf.:* <https://www.decolar.com/passagens-aereas/rio/sao/passagens-aereas-para-sao+paulo-saindo-de-rio+de+janeiro?priceDate=MjAyMi0xMS0yNVQyMjo1Mjo0Mi40MjgzNDJaW1VUQ10%3D&airlines=AD&clickedPrice=BRL_408&refererEvent=VR>. Acesso em 25 nov. 2022.

[121] GRAY, Colin M.; et. al. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI'18. ACM, New York, NY, USA, Article 534, 2018, p. 14.

[122] Segundo a Autoridade Nacional de Proteção de Dados, "cookies são arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas". Vide: AUTORIDADE NACIONAL DE PROTEÇAO DE DADOS. Guia Orientativo: Cookies e proteção de dados pessoais, publicado em outubro de 2022. Brasília, 2022. Disponível em: < https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em 20 nov. 2022.

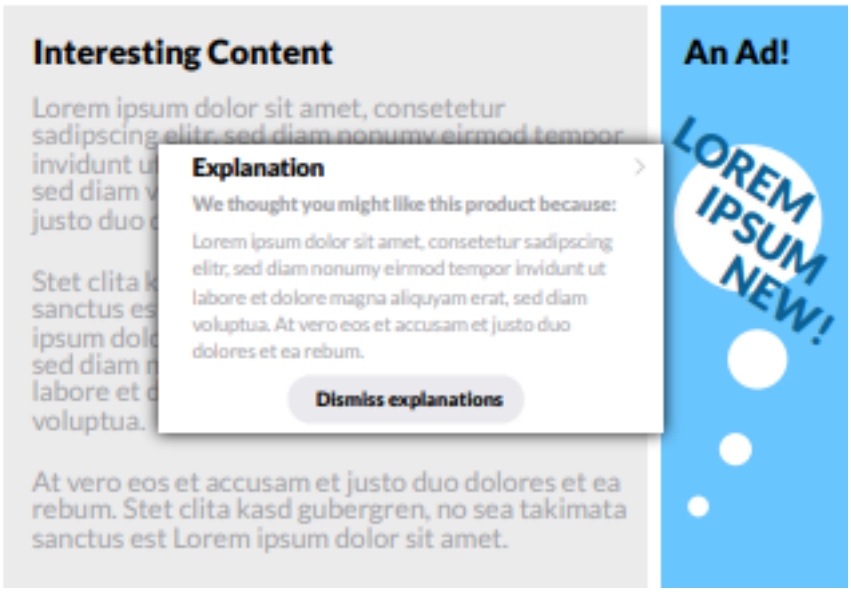


Figura 9: Exemplo hipotético de interface de *dark pattern* de evasão em que usuários são encorajados a dispensar explicações, uma vez que é disponibilizada cobrindo o conteúdo principal do site (Fonte: CHROMIK et al. *Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems*, Los Angeles: IUI Workshops n. 19, 2019, p.4)

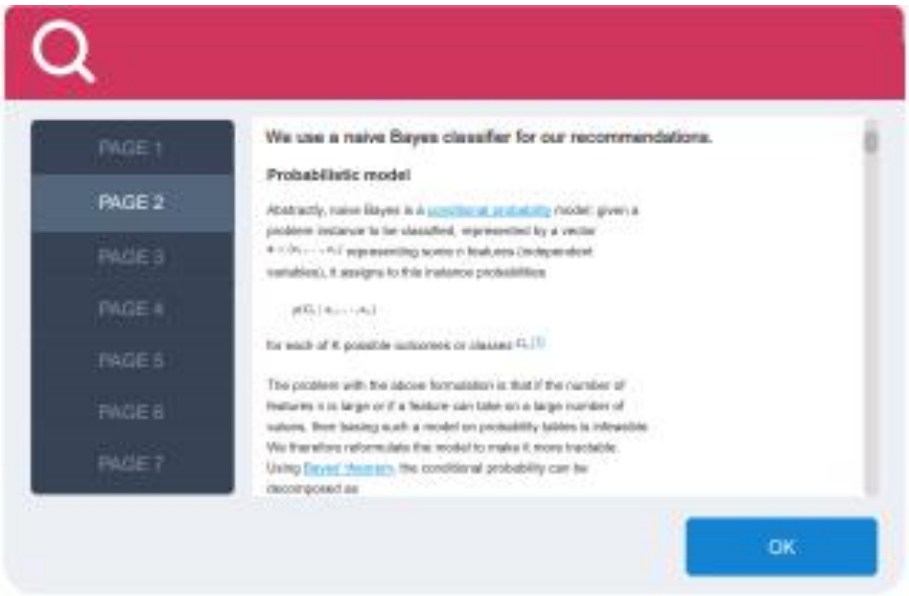
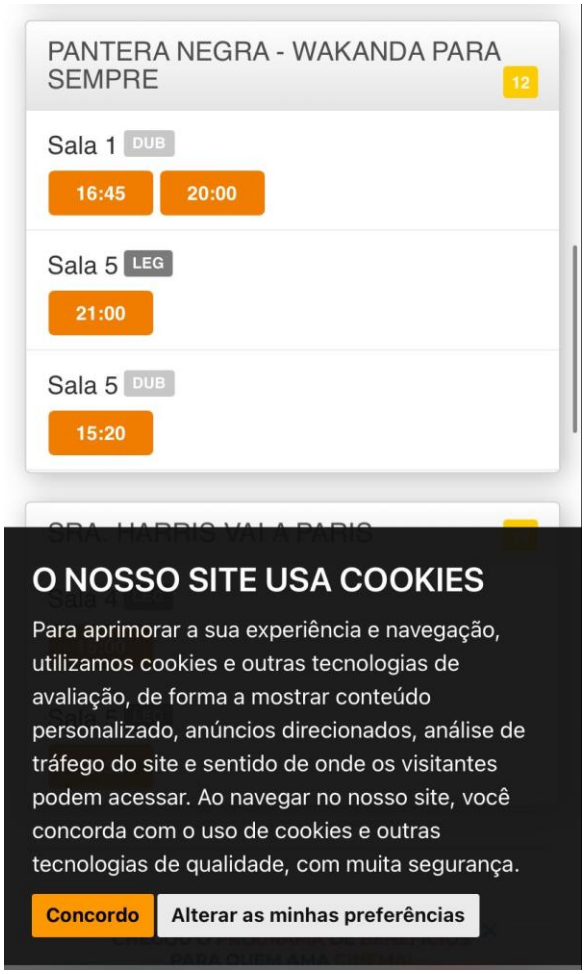
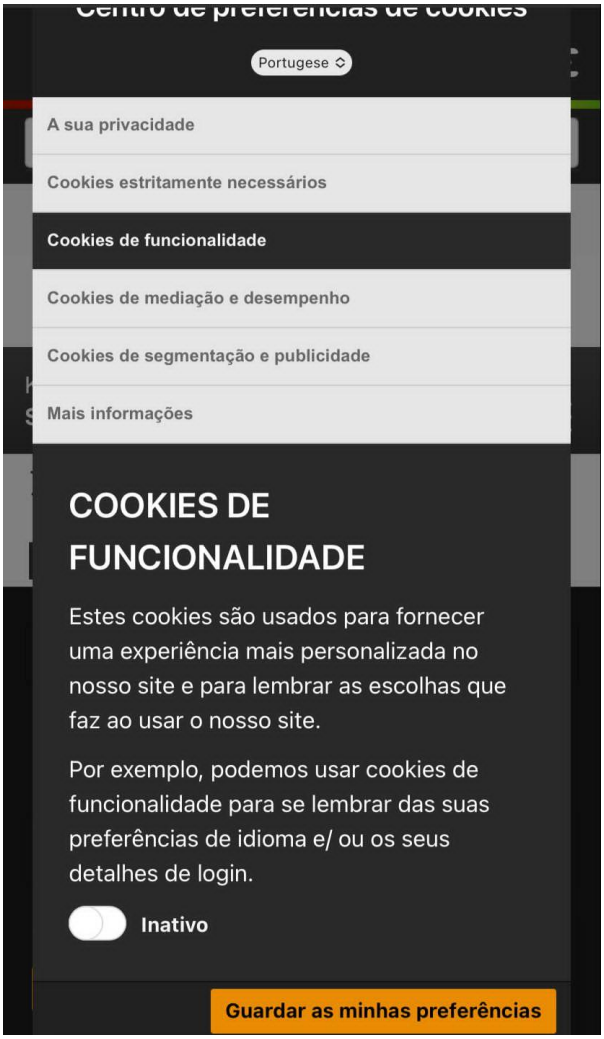


Figura 10: Exemplo hipotético de *dark pattern* de evasão em que é dada uma sobrecarga de informação técnica para titulares de dados a fim de obter seu consentimento com termos de uso ou políticas de privacidade de determinada plataforma ou cookies (Fonte: CHROMIK et al. *Op. cit.*, 2019, p. 4)


PANTERA NEGRA - WAKANDA PARA SEMPRE
12
Sala 1
DUB
16:45
20:00
Sala 5
LEG
21:00
Sala 5
DUB
15:20
O NOSSO SITE USA COOKIES
Para aprimorar a sua experiência e navegação, utilizamos cookies e outras tecnologias de avaliação, de forma a mostrar conteúdo personalizado, anúncios direcionados, análise de tráfego do site e sentido de onde os visitantes podem acessar. Ao navegar no nosso site, você concorda com o uso de cookies e outras tecnologias de qualidade, com muita segurança.
Concordo
Alterar as minhas preferências



Figuras 11 e 12: Caso concreto de *dark pattern* de evasão em que a interface para alteração de preferência de *cookies* impede o titular de dados de visualizar o conteúdo principal do site, além de se apresentar em diversas seções (conferindo sobrecarga de informações), motivando-o a dispensar a informação trazida pela política proposta. (Fonte: edição da autora)[123]

Não é incomum que os usuários de plataformas digitais e *big techs* tenham se deparado com todos os tipos de *dark patterns* mencionados neste capítulo, visto serem os mais empregados pelas empresas de tecnologia para manipular o processo decisório de seus consumidores. As consequências que tais técnicas manipulatórias trazem aos titulares de dados são variadas, tendo repercussão relevante, para fins deste trabalho, na seara jurídica e psicológica.

[123] Cf: <https://kinoplex.com.br/cinema/kinoplex-terraco-shopping/12?query=pantera%20ne>. Acesso em: 25 nov. 2022.

Quanto ao campo jurídico, os impactos nos direitos relativos à proteção de dados, privacidade, autodeterminação informativa e os de âmbito consumerista serão melhor elucidados na seção II deste trabalho. Em contrapartida, por ora, vale destaque à principal repercussão na esfera psíquica dos indivíduos submetidos às *dark patterns*: a **dissonância cognitiva**.

A dissonância cognitiva é o resultado de um estado psicológico incômodo, solucionado pelo consumidor a partir da reorganização da sua própria estrutura cognitiva.[124] Isso porque a **Teoria da Dissonância Cognitiva**, fundada por Leon Festinger, pressupõe que o indivíduo necessitaria sempre de estabelecer o equilíbrio entre os componentes da sua atitude para alcançar a sua consistência.[125]

Um excelente exemplo disso seria no momento em que um consumidor, ao ser influenciado a adquirir um produto que, em um primeiro momento, não gostaria de tê-lo adquirido, viu-se persuadido a comprá-lo por uma *dark pattern* de isca e troca. Segundo a referida teoria, esse consumidor, após a compra indesejada, entrará em dissonância cognitiva e, a fim de estabelecer novamente a consistência cognitiva, tentará se convencer de que a compra realizada foi correta ou de que realmente necessitava do produto. Neutzlig Fraga converge no mesmo sentido ao afirmar que:

> Esse fato é evidenciado especialmente na dissonância cognitiva pós-compra, situação na qual as possibilidades ignoradas num primeiro momento (informações sobre o produto/marca) subitamente se tornam pertinentes e interessantes, surgindo então inúmeras dúvidas quanto à escolha já efetuada. Essa dissonância tende a ser dissipada por meio de mecanismos psicológicos, como por exemplo, o de apoio à escolha efetuada ou o da busca por informações que confirmem sua suposta validade.[126]

Cass Sunstein também já discorreu a respeito da dissonância cognitiva, ao expor que "as pessoas tentam reduzir a dissonância cognitiva se negando a acreditar em afirmações que contradizem suas crenças mais enraizadas".[127] Dessa feita, o autor não apenas corrobora com o

---

[124] Conceituação extraída do estudo de: NEUTZLING FRAGA, P. *Atitude do Consumidor: o Caminho para a Persuasão*, VIII Congresso Brasileiro de Ciências da Comunicação da Região Sul, Passo Fundo, RS: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007.

[125] FESTINGER, Leon A. *A theory of cognitive dissonance*, Evanston, II: Row. Peterson, 1957.

[126] NEUTZLING FRAGA. *Op. cit*., 2007, p. 10.

[127] SUNSTEIN, Cass R. *A verdade sobre os boatos*: como se espalham e por que acreditamos neles. Rio de Janeiro: Elsevier, 2010, p. 24.

que Leon Festinger já anunciava na década de 50, mas também comprova que o componente emocional na assimilação de informações é um fator diferencial na "sociedade de vigilância".[128]

Logo, *(hiper)nudges* e *dark patterns* guardam intrínseca relação entre si, visto ambos serem técnicas que manipulam diretamente o titular de dados a tomar decisões (ou não) diferentes das previamente determinadas pelo mesmo. As consequências que essas técnicas manipulatórias trazem aos usuários e consumidores inseridos no contexto digitalizado se dão em diversas searas, incluindo em seus direitos e em sua *psique*. No que tange ao campo psíquico, importa destacar a dissonância cognitiva ocasionada aos consumidores submetidos a tais práticas persuasivas, devido à assimilação de informações estar ligada a forte viés emocional em busca de consistência e equilíbrio dos componentes de suas ações.

Além da Economia Comportamental, outra área da ciência que auxilia na compreensão dos processos de manipulação dos titulares de dados no capitalismo datificado é a Economia Psíquica dos Algoritmos, que será discorrida no próximo subcapítulo.

3.2 – A Economia Psíquica dos Algoritmos: modelo do gancho, psicometria e matematização de expressões faciais

Como visto no subcapítulo anterior, a *Behavioral Economics* demonstra que os indivíduos possuem limitações de racionalidade e influências de emoções e vieses[129] que comprometem significativamente o livre exercício de seus direitos de liberdade, autodeterminação informativa, privacidade e proteção de dados pessoais, garantidos no ordenamento jurídico brasileiro, corroborados com a vigência da Lei Geral de Proteção de Dados, a partir de 2018 (vide seção II).

Novamente, cabe frisar que Frank Pasquale, dentre diversos outros autores, afirma que os controladores de dados pessoais não focam em tratar adequadamente os dados dos titulares – respeitando suas garantias constitucionais e infraconstitucionais –, mas sim em maximizar

[128] A nomenclatura é dada pelo próprio autor – SUNSTEIN. *Op. cit*., 2010, p. 83.

[129] FRAZÃO, Ana. Proteção de dados pessoais e democracia: a ameaça da manipulação informacional e digital. In: *A Lei Geral de Proteção de Dados LGPD*. Revista dos Tribunais, 2021, pp. 739-762.

seus lucros,[130] independentemente das consequências negativas que essa conduta possa trazer àqueles cujos dados foram fornecidos.

Diante disso, o fenômeno de investimento em processos algorítmicos de captura, produção e análise de informação – extraída de dados – é denominado **Economia Psíquica dos Algoritmos.**[131] O investimento se realiza em diversas áreas, dentre elas a tecnocientífica, a econômica e a social; bem como em diferentes dispositivos e serviços, a exemplo de mídias sociais, aplicativos, serviços de *streaming* e plataformas digitais. Toda a aplicação de capital é voltada a modular comportamentos com fins de maximizar a lucratividade empresarial em detrimento de garantias, direitos e bem-estar dos consumidores.

Dentro da Economia Psíquica dos Algoritmos, há duas subdivisões de matrizes manipulatórias comportamentais: **a matriz da captura (captológica) e a matriz da predição (preditiva)**. A primeira diz respeito à captologia e ao engajamento de informações, tendo relação intrínseca com a economia da atenção,[132] e a segunda refere-se à predição de comportamentos e à vulnerabilidade dos consumidores, como será demonstrado adiante.

3.2.1 – Matriz captológica

A matriz captológica é o conjunto de tecnologias manipulatórias empregado para capturar, direcionar e mobilizar a atenção dos usuários[133] de plataformas digitais e *big techs* pelo máximo de tempo possível. A captologia tem como base a teoria de B.J. Fogg – fundador do Laboratório de Tecnologias Persuasivas em Stanford –, cujo destaque se deu em pesquisas práticas e teóricas com objetivo de elucidar uma intersecção entre tecnologias computacionais e persuasão, visando efeitos planejados.[134]

---

130 PASQUALE. *Op. cit.*, 2015.

131 BRUNO, Fernanda Glória. *A economia psíquica dos algoritmos:* quando o laboratório é o mundo. NEXO Jornal, Brasil, pp. 1-3, 12 jun. 2018.

132 A definição de "economia da atenção" será dada no tópico "3.2.1 - Matriz captológica".

133 SANTOS, Isabela de Araújo. *Manipulação comportamental em uma economia datificada:* uma análise de métodos de persuasão da psicologia para obtenção de dados no capitalismo de vigilância, publicado em 03 mar. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/comportamento-manipulacao-comportamental-na-economia-datificada-03032022>. Acesso em 21 nov. 2022.

134 FOGG, Brian J. *A Behavior Model for Persuasive Design*, Persuasive Technology Lab Stanford University, 2009.

É notável, dessa feita, a proximidade da captologia com a Psicologia Behaviorista, visto ambas analisarem aspectos de influência no comportamento humano, de maneira a obter padrões desejados ao prever e controlar ações. Shoshana Zuboff, inclusive, reconhece, em certa medida, que o capitalismo de vigilância cria uma arquitetura behaviorista propícia à atuação veemente e em ampla escala das *big techs*.[135]

Essa atuação se dá por meio do investimento na denominada economia da atenção, que seria uma estrutura econômica de ferramentas analíticas e práticas[136] que considera a atenção humana como um bem escasso. Isso porque parte-se do pressuposto de que se hoje, com todas as disrupções tecnológicas existentes, "há uma superabundância de conteúdos visuais, informacionais e interativos, [...] o que falta é justamente atenção (e tempo) para acessar e consumir todo este oceano de ofertas".[137]

Diante disso, Nir Eyal propõe métodos e etapas de alto nível de resultado prático para empreendedores que almejam capturar a atenção de seus consumidores e tornar seus produtos cada vez mais atraentes aos mesmos, a partir da criação do "modelo do gancho",[138] "que objetiva estimular a criação de hábitos de consumo".[139]

O "modelo do gancho" é dividido em quatro etapas**: i) gatilhos** – que se subdividem em externos e internos –, **ii) ação**, **iii) recompensas variáveis** e **iv) investimento**. Analisemos, a seguir, cada uma delas.

1) A primeira etapa constitui-se nos chamados "**gatilhos**", que seriam estímulos que despertam algum comportamento desejado, comparativamente à teoria behaviorista, poderíamos compará-los com os condicionamentos operantes.[140] Os gatilhos se subdividem em **externos e internos**: os primeiros seriam quaisquer fenômenos que chamassem a atenção do usuário ou consumidor à ação - a exemplo de notificações

---

[135] SANTOS. *Op. Cit.*, 2022.

[136] CALIMAN, Luciana Vieira. *A biologia moral da atenção*: a constituição do sujeito (des)atento. Tese de Doutorado em Saúde Coletiva, Universidade do Estado do Rio de Janeiro, Instituto de Medicina Social, Rio de Janeiro, 2006.

[137] BENTES, Anna. *A gestão algorítmica*: enganchar, conhecer e persuadir. Políticas, Internet e Sociedade, Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2019, p. 227.

[138] EYAL, Nir; HOOVER, Ryan. *Hooked:* How to Build Habit-Forming Products, Portfolio Penguin, 2014.

[139] SANTOS. *Op. Cit.*, 2022.

[140] Os condicionamentos operantes são os processos voluntários em que o sujeito "opera" sobre o meio, de modo a gerar consequências (notadamente reforços ou punições) e mudanças no ambiente. – *Cf.*: BARBOSA, Katiuscia de Azevedo et al. *A técnica de condicionamento operante dentro do laboratório*, João Pessoa: X Encontro de Iniciação à Docência, UFPB-PRG, 2007.

chamativas, normalmente na cor vermelha, nos *smartphones* a fim de "enganchar"[141] o indivíduo nos aplicativos –; e os últimos seriam emoções – em sua maioria negativas – que impulsionariam os usuários a retornar às redes, como o tédio, a tristeza e até mesmo a raiva.[142]

2) A segunda etapa é designada "**ação**", que consiste na análise do comportamento adotado pelos usuários diante dos gatilhos. A ação, para ser eficaz, deve ser fácil e acessível, a fim de que o agir venha como uma atitude automática, um **hábito**.[143] Além disso, insta salientar que esse hábito criado com fins econômicos favorece o monopólio das plataformas digitais e *big techs*; afinal essa otimização de tempo e tarefa dos seus usuários – se tornando quase um costume – estimula-os a permanecer fisgados em seus serviços, isto é, utilizando-os por mais tempo. Nesse sentido, vale rememorar o conceito de Richard Thaler e Cass Sunstein referente ao *nudge*, que seria um "empurrãozinho", um aspecto da arquitetura de escolha capaz de mudar e direcionar o comportamento humano, sem proibir nenhuma opção ou alterar significativamente seus estímulos econômicos. Por meio da utilização do *nudge*, as grandes plataformas facilitam o acesso aos seus conteúdos, incentivando os seus usuários a permanecerem por mais tempo, com maior atenção, ao que lhes é disponibilizado.

3) A terceira etapa do modelo do gancho para captura da atenção é chamada de "**recompensas variáveis**", que se aproxima muito dos experimentos behavioristas - especialmente aos realizados por B. F. Skinner, ao inserir variabilidade de recompensas por determinado comportamento.[144] Nessa etapa, desta feita, parte-se do pressuposto de que a existência de grande variedade de recompensas aumentaria significativamente o comportamento desejado: "a *timeline* das plataformas digitais

[141] A terminologia de "enganchar" usuários é usualmente utilizada pela professora Anna Bentes, aludindo à teoria do gancho de Eyal. Vide: BENTES, Anna. *Quase um tique*: economia da atenção, vigilância e espetáculo em uma rede social, Rio de Janeiro: Ed. UFRJ, 2021.
[142] SANTOS. *Op. Cit.*, 2022.
[143] Eyal parte da premissa de que, para algumas empresas, a formação de hábitos é essencial para sua própria existência, visto competir constantemente pela atenção de seus consumidores em um meio de infinitas distrações: "For many products, forming habits is an imperative for survival. As infinite distractions compete for our attention, companies are learning to master novel tactics to stay relevant in users' minds." – EYAL; HOOVER. Op. cit., 2014, p. 6.
[144] ZANATTA, Rafael. A. F.; ABRAMOVAY, Ricardo. *Dados, vícios e concorrência: repensando o jogo das economias digitais*. Estudos Avançados, [S. l.], v. 33, n. 96, 2019.

[se] tornaram, em certa medida, variáveis e imprevisíveis".[145] O conteúdo que será trazido ao usuário tem inúmeras possibilidades de apresentação, além de que, quando combinado com os algoritmos utilizados por essas empresas a fim de incrementar a publicidade direcionada, os usuários sentem-se – mesmo que involuntariamente – compelidos a acessarem as plataformas, de maneira a buscar cada vez mais as recompensas oferecidas, que se apresentam em três principais facetas: i) **recompensas sociais** (*rewards of the tribe*) – que seriam os reforços positivos obtidos através da aprovação da comunidade[146] –; ii) **recompensas da caça** (*rewards of the hunt*) – as quais estariam ligadas à persecução de recursos e informações bem sucedida[147] –; e iii) **recompensas pessoais** (*rewards of the self*) – relacionadas a gratificações de cada indivíduo ao superar obstáculos.[148] Eyal resumiu a tríade de recompensas da seguinte maneira, para demonstrar que muitas vezes podem ser oferecidas ao consumidor em concomitância com as outras:

Figura 13: Tríade de recompensas da terceira etapa do modelo do gancho. (Fonte: EYAL, Nir; HOOVER, Ryan. *Hooked:* How to Build Habit-Forming Products, Portfolio Penguin, 2014)

4) Por fim, Eyal sugere que a quarta e última etapa seria o "**investimento**" das empresas em mais mecanismos de captura da atenção, de maneira a perpetuar e

[145] SANTOS. *Op. Cit.*, 2022.
[146] EYAL; HOOVER. Op. cit., 2014, p. 70.
[147] *Ibid.*, p. 74.
[148] *Ibid.*, p. 77.

aprimorar gradualmente a matriz captológica da economia da atenção. Com isso, tem-se a dinâmica cíclica do modelo do gancho, esquematizada a seguir:

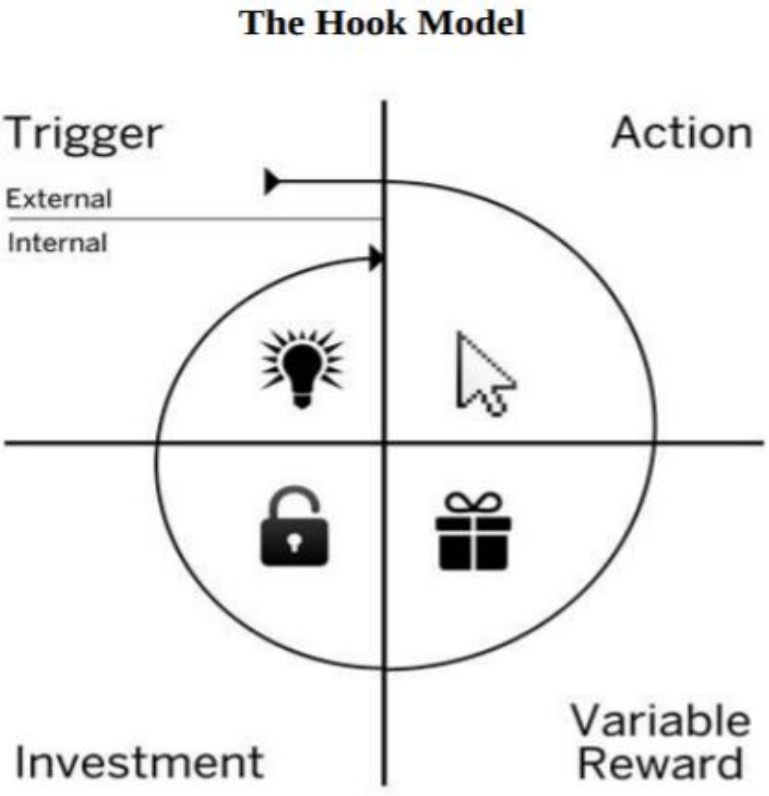


Figura 14: Modelo do gancho esquematizado (Fonte: EYAL; HOOVER. Op. cit., 104, p. 9)

Nesse sentido, pode-se afirmar que esse modelo de engajamento de usuários em hábitos de consumo cíclicos e impulsivos coaduna-se intrinsecamente com o ideal de comportamento dos consumidores almejado no capitalismo de vigilância datificado, por justamente incentivar um sistema de estímulos e recompensas, de modo a fomentar a disponibilização de seus dados pessoais às empresas que se utilizam desses métodos captológicos. Portanto, sob o prisma econômico, o modelo do gancho de Eyal é extremamente eficiente para o fim que se propõe alcançar, principalmente em uma sociedade que vem priorizando técnicas manipulatórias em detrimento de salvaguardas aos consumidores – vide seção II.

Um bom exemplo que comprova a alta eficiência do modelo do gancho, é uma pesquisa realizada em 2019, sobre vícios ligados a *smartphones*, em que foi demonstrado que o usuário

médio de *smartphone* nos Estados Unidos checa seu dispositivo 63 vezes por dia, e essa quantidade vem aumentando a cada ano. Além disso, 85% das pessoas checam seus telefones enquanto estão conversando com amigos e familiares, bem como 69% dos usuários checam seus celulares em até cinco minutos depois que acordam (antes mesmo de realizar qualquer outra atividade), e 87% fazem-no logo antes de dormir. Por fim, foi identificado que 58% dos usuários tentaram mudar seus hábitos, mas apenas 41% dessas tentativas foram bem-sucedidas.[149] Esse estudo valida, em certa medida, a terceira etapa do modelo do gancho, por exemplificar como o sistema de recompensas do cérebro é estimulado pelo uso constante de *smartphones* e, consequentemente, das plataformas digitais disponíveis em seu *software*.

Daí por que nesse contexto, tanto para Skinner,[150] quanto para Zuboff,[151] a liberdade humana não passa de ilusão e exprime nada mais do que nosso desconhecimento sobre os mecanismos determinantes de nossas ações. Tal máxima se aplica adequadamente a um contexto de alto fluxo de dados pessoais, escavação de emoções e uso de relações sociais como principal matéria prima das plataformas digitais e *big techs.*[152]

Isso porque, como visto no subcapítulo 3.1, a sensação de liberdade de escolha está, na realidade, condicionada a estímulos – *nudges* – e recompensas momentâneas que exigem uma hiperatenção dos consumidores, a ponto de muitas vezes serem compelidos a tomar atitudes de maneira irracional – e até mesmo prejudicial – a fim de atender às demandas de mercado e às imposições sociais de alta celeridade exigidas na sociedade de vigilância.

Enquanto o discurso apresentado aos consumidores vigiados pelas empresas vigilantes foca consideravelmente na liberdade de escolha – apresentando-lhes termos de uso e políticas de privacidade pautadas em um suposto consentimento livre, inequívoco e informado (vide seção II) –, bem como na **consideração destes como sujeitos racionais e perfeitamente informados**; a realidade é que essas empresas vêm explorando cada vez mais a **vulnerabilidade cognitiva e emocional** de sujeitos considerados, de acordo com o que foi elucidado até aqui, como **impulsivos e suscetíveis à persuasão**.

---

[149] TURNER, Ash. *Smartphone addiction facts & phone usage statistics the definitive guide* (2020-2021 Update) Disponível em: < https://www.bankmycell.com/blog/smartphone-addiction/#chap-ter0 >. Acesso em 23 nov. 2022.

[150] SKINNER, Burrhus F. *Para além da liberdade e da dignidade*. Lisboa: Edições 70, 2000.

[151] ZUBOFF, S. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

[152] SANTOS. *Op. Cit.*, 2022.

Veremos, em seguida, que o engajamento (e enganchamento) dos usuários não é a única vertente da Economia Psíquica dos Algoritmos capaz de vulnerabilizá-los. O investimento em tecnologias de predição dos seus comportamentos constitui hoje também uma das principais formas de manipulação das suas tomadas de decisão, repercutindo em diversas violações emocionais e sentimentais.

3.2.2 – Matriz preditiva

A matriz preditiva é a arquitetura de tecnologia da Economia Psíquica dos Algoritmos responsável por extrair dados pessoais por métodos de reconhecimento de "emoções medidas pela precisão do acerto, seja pela personalidade do usuário ou consumidor, seja [pelos] aspectos psicológicos e emocionais apresentados momentaneamente".[153]

A predição de comportamentos empregadas por essas tecnologias é baseada em grande parte no método da psicometria de Michal Kosinski – notadamente contida no campo de estudo da Psicologia Cognitiva –, cuja inspiração se deu no modelo do Big Five, cunhado por Lewis Goldberg no início da década de 80. Em uma tradução literal, o Modelo dos Cinco Fatores se propõe a identificar cinco principais traços personalísticos de um indivíduo através de quatro hipóteses: lexical, empirismo, análise fatorial e universalidade.[154]

Os cinco fatores abordados por Goldberg são: abertura, extroversão, consciencialidade, condescendência e neuroticismo. Cada um desses fatores revelaria algum traço de personalidade capaz de ser utilizado, a partir do modelo de psicometria de Kosinski, para predizer comportamentos dos usuários de *big techs* a partir de técnicas de perfilização – *profiling* (vide capítulo 2 para definição).

O estudo de Kosinski revelou que, quando combinadas várias características, em especial a extroversão com as demais, torna-se possível realizar previsões relativamente precisas em relação à personalidade de cada indivíduo.[155] Analisando, portanto, as informações extraídas das mídias sociais, seria possível perfilar esses usuários, dividindo-os automaticamente em diferentes segmentos e adaptando os anúncios a cada um deles, com base

---

[153] *Idem.*

[154] GOLDBERG, Lewis R. *The structure of phenotypic personality traits*. American psychologist, v. 48(1), n. 26, 1993.

[155] BACHRACH, Yoram et al. Personality and patterns of Facebook usage. *In: Proceedings of the 4th annual ACM web science conference*, 2012, pp. 24-32.

em sua personalidade. Logo, não seria necessária nem mesmo a realização de testes de personalidade disponíveis nas plataformas digitais, pois seus próprios comportamentos *online* já revelariam muitos traços personalísticos previsíveis.

Ainda de acordo com a referida pesquisa de Kosinski, a abertura e o neuroticismo estão positivamente relacionados com o número de atualização de *status*, fotos, grupos e curtidas de um usuário de plataformas digitais. Ademais, a realização pessoal – relacionada à consciencialidade – estaria negativamente ligada a todos os aspectos do uso da plataforma do Facebook – número de amigos, curtidas, fotos etc. –, bem como a extroversão estaria diretamente relacionada ao uso constante da plataforma. Por fim, foi constatado que a socialização – associada à condescendência – seria proporcionalmente correlacionada com o número de amigos, grupos e curtidas.[156] Vejamos os principais resultados levantados por Kosinski em formato esquematizado:

Personality Trait	Profile Feature	Pearson Correlation
Openness	Likes	0.102
	Statuses	0.062
	Groups	0.077
Conscientiousness	Likes	-0.088
	Groups	-0.0697
	Photos	0.0330
Extraversion	Statuses	0.117
	Likes	0.034
	Groups	0.069
	Friends	0.177
Agreeableness	Likes	-0.036
Neuroticism	Likes	0.075
	Friends	-0.059

Table 2. Statistically significant correlations between personality traits Facebook profile features (at a significance level of $p < 1\%$).

Figura 15: Correlação entre tipos de personalidade e fatores psicométricos, sendo as correlações relevantes $p < 1\%$, sendo p = Pearson Correlation. (Fonte: BACHRACH, Yoram et al. Personality and patterns of Facebook usage. *In: Proceedings of the 4th annual ACM web science conference*, 2012, p. 31)

[156] *Idem.*

Em diferente estudo, Kosinski e sua equipe demonstraram ainda que registros digitais de comportamento facilmente acessíveis, a exemplo dos *likes* no Facebook, podem ser utilizados para prever de forma automática e precisa uma variedade de atributos e informações pessoais altamente sensíveis,[157] incluindo orientação sexual, etnia, religião, posicionamento político, traços de personalidade, felicidade, inteligência, idade e sexo.[158]

Cabe citar ainda o artigo publicado por Ruben Van de Ven em 2015, em que o autor averiguou que os *likes* do Facebook poderiam indicar mais informações sobre uma pessoa do que uma relação de parentesco, de amizade e de trabalho poderia revelar sobre o mesmo indivíduo.[159] Dessa pesquisa pode-se notar, inclusive, a eficiência dos *softwares* de análise de emoções, que traduzem expressões faciais em parâmetros quantificados, permitindo comparações estatísticas entre personalidades.

O psicanalista francês Franck Enjolras vai ao encontro dessa perspectiva ao constatar que os dados extraídos de *posts*, *likes*, movimentos, fotos e compras dos usuários de plataformas digitais permitem aos algoritmos um conhecimento dos titulares de dados capaz de não só saber o que fazem ou o que fizeram, mas também o que farão.[160] No mesmo sentido, Zanatta e Abramovay pontuam que:

> (...) o inconsciente se revela não na sessão de psicanálise, na relação vivida entre dois seres humanos, de forma íntima, discreta e com a finalidade de ampliar nosso autoconhecimento, mas por dispositivos controlados por estruturas que coletam, armazenam e analisam nossos mais elementares gestos cotidianos e que dão concretude à ideia, hoje já banal, de que os algoritmos nos conhecem melhor que nós mesmos ou que as pessoas com quem convivemos em laços estreitos.[161]

Tais dispositivos são justamente os *softwares* mencionados por Van de Ven em sua pesquisa, cuja operacionalização se dá pela análise das emoções, exercendo um *feedback* subconsciente objetivo e concomitante com a própria expressão facial detectada dos indivíduos.

---

[157] KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. *Private traits and attributes are predictable from digital records of human behavior*, PNAS, Washington, DC, v. 110, n. 15, pp. 5802-5805, 2013.
[158] Exemplos trazidos por: SANTOS, *Op. Cit.*, 2022.
[159] VAN DE VEN, Ruben. *Emotion Analysis Software*: *Choose How You Feel; You Have Seven Options*, Institute of Network Cultures, 2017. Disponível em: <https://networkcultures.org/longform/2017/01/25/choose-how-you-feel-you-have-seven-options/>. Acesso em 21 nov. 2022.
[160] ENJOLRAS, Franck. *Gare à ces 'algorithmes qui pourraient finir par nous connaître mieux que nous nous connaissons nous-mêmes'*. Le Monde, publicado em 26 dez. 2018. Disponível em: <https://www.lemonde.fr/sciences/article/2017/12/26/gare-a-ces-algorithmes-qui-nous-connaissent-mieux-que-nous-memes_5234390_1650684.html#:~:text=Par%20leur%20analyse%2C%20des%20algorithmes,mettre%20fin%20%C3%A0%20nos%20jours.>. Acesso em: 15 jun. 2019
[161] ZANATTA; ABRAMOVAY. *Op. cit*., 2019, p. 425.

Os rostos identificados por esses sistemas operacionais são convertidos em sete padrões numéricos, similares às sete expressões universais de emoção descritas pelo psicólogo Paul Ekman:[162] raiva, repulsa, desprezo, alegria, medo, surpresa e tristeza.[163]

A teoria de Ekman foi revisitada pela psicóloga Lisa Feldman Barrett em artigo mais recente, cujo escopo constituiu em demonstrar a possibilidade de realizar uma padronização universal das expressões faciais de acordo com cada sentimento demonstrado pelos indivíduos, bem como a possibilidade de **matematização e codificação dessas expressões faciais**.[164] Essa objetivação da subjetividade possibilitou às empresas de tecnologia um enorme poder de influência e predição comportamental humana sobre seus consumidores. Isso porque a identificação e previsão de reações comportamentais se concretiza em melhor engajamento econômico das próprias plataformas digitais e *big techs*, ao oferecerem conteúdos e produtos direcionados para cada usuário.

Para que possamos entender como se dá a matematização e codificação de expressões por meio dos algoritmos utilizados por *softwares*, cabe destacar alguns dos resultados da pesquisa de Barrett. A psicóloga analisou diversas fontes para categorizar reações humanas distintas em "unidades de ação" ("*action units"*[165]), que correspondem a uma área do rosto de um indivíduo. Assim, sistematizou em seu estudo os estados emocionais relativos a cada expressão da seguinte maneira:

[162] Vide: EKMAN, Paul. Universals and Cultural Differences in Facial Expressions of Emotions. *In:* COLE, J. (Ed.), *Nebraska Symposium on Motivation*, v. 19, Lincoln, NB: University of Nebraska Press, 1972, pp. 207-282.
[163] VAN DE VEN, *Op. cit*., 2017.
[164] Também abreviadas como AU's – BARRETT, Lisa Feldman et al. *Emotional expressions reconsidered:* Challenges to inferring emotion from human facial movements. Psychological science in the public interest, v. 20, n. 1, 2019, pp. 1-68.
[165] BARRETT et al. *Op. cit.*, 2019, p. 7.

State	Example Photo	Action Units	Physical Description
Amusement		6 + 7 + 12 + 25 + 26 + 53	Head back, Duchenne smile, lips separated, jaw dropped
Anger		4 + 5 + 17 + 23 + 24	Brows furrowed, eyes wide, lips tightened and pressed together
Boredom		43 + 55	Eyelids drooping, head tilted (not scorable with FACS: slouched posture, head resting on hand)
Confusion		4 + 7 + 56	Brows furrowed, eyelids narrowed, head tilted
Contentment		12 + 43	Smile, eyelids drooping
Coyness		6 + 7 + 12 + 25 + 26 + 52 + 54 + 61	Duchenne smile, lips separated, head turned and down, eyes turned opposite to head turn
Desire		19 + 25 + 26 + 43	Tongue shown, lips parted, jaw dropped, eyelids drooping
Disgust		7 + 9 + 19 + 25 + 26	Eyes narrowed, nose wrinkled, lips parted, jaw dropped, tongue shown
Embarrassment		7 + 12 + 15 + 52 + 54 + 64	Eyelids narrowed, controlled smile, head turned and down (not scorable with FACS: hand touches face)

State	Example Photo	Action Units	Physical Description
Fear		1 + 2 + 4 + 5 + 7 + 20 + 25	Eyebrows raised and pulled together, upper eyelid raised, lower eyelid tense, lips parted and stretched
Happiness		6 + 7 + 12 + 25 + 26	Duchenne smile
Interest		1 + 2 + 12	Eyebrows raised, slight smile
Pain		4 + 6 + 7 + 9 + 17 + 18 + 23 + 24	Eyes tightly closed, nose wrinkled, brows furrowed, lips tight, pressed together, and slightly puckered
Pride		53 + 64	Head up, eyes down
Sadness		1 + 4 + 6 + 15 + 17	Brows knitted, eyes slightly tightened, lip corners depressed, lower lip raised
Shame		54 + 64	Head down, eyes down
Surprise		1 + 2 + 5 + 25 + 26	Eyebrows raised, upper eyelid raised, lips parted, jaw dropped
Sympathy		1 + 17 + 24 + 57	Inner eyebrow raised, lower lip raised, lips pressed together, head slightly forward

Figura 16: Variações de 22 expressões faciais em pessoas de cinco culturas distintas. (Fonte: BARRETT, Lisa Feldman et al. *Emotional expressions reconsidered:* Challenges to inferring emotion from human facial movements. Psychological science in the public interest, v. 20, n. 1, 2019, p. 7)

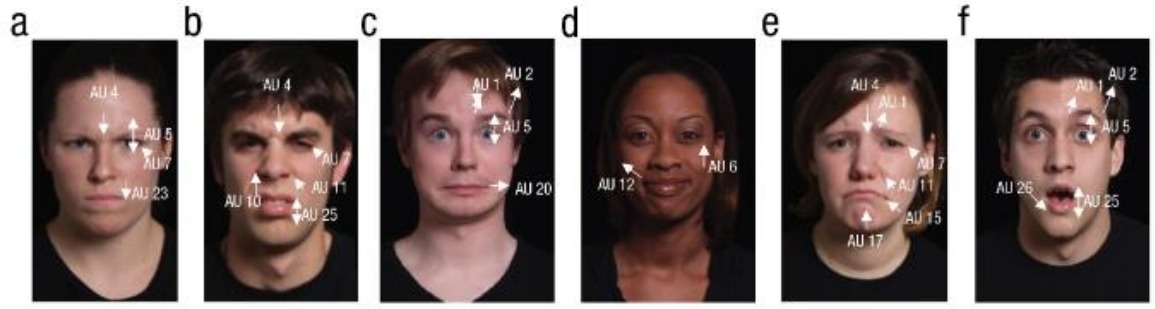


Figura 17: A expressão "a", com suas respectivas AUs, corresponde à emoção raiva; "b", ao nojo; "c", medo; "d", à "alegria"; "e", à tristeza; e "f" à surpresa. (Fonte: BARRET et al. *Op. cit.*, 2019, p. 13)

A partir dessa análise matemática da subjetividade humana, Barrett averigou dois principais pontos que merecem destaque: i) em primeiro lugar, companhias de tecnologia investem demasiado capital em engenharia de *software* para leitura de expressões faciais;[166] ii) por fim, mas não menos importante, essa tecnologia não lê emoções, mas sim movimentos do rosto humano.[167]

Essa última constatação foi essencial para que plataformas digitais e *big techs*, bem como outras companhias vigilantes do mundo digitalizado, passassem a se engajar em outros tipos de tecnologias para adentrar ainda mais no âmbito emocional e introspectivo dos seus consumidores e usuários. Assim, recorreram à Neurociência para tanto, já que esta fornece-lhes mecanismos mais eficientes de detecção de reações humanas, processos fisiológicos e dados cerebrais precisos. Passemos, portanto, à sua elucidação.

3.3 – A Neurociência: *neuromarketing*, pesquisas invasivas e aprimoramento da manipulação

Além de contar com a Economia Comportamental e com a Economia Psíquica dos Algoritmos, o capitalismo de vigilância datificado se apoia na Neurociência para manipular consciências, visto o nível de intrusividade nos processos neurofisiológicos humanos possibilitados por esse campo científico. Hoje, processos decisórios de compra não são mais tomados conscientemente: segundo Billy Nascimento,[168] as tomadas de decisão por parte dos

[166] BARRET et al. *Op. cit,* 2019, p. 47.
[167] *Idem.*
[168] Doutor em Neurofisiologia pela Universidade Federal do Rio de Janeiro e fundador da Forebrain, empresa de pesquisas em neurociência aplicada ao marketing.

consumidores ocorrem em média em até dois segundos e há uma influência determinante de processos cognitivos automáticos, principalmente de emoções.[169]

"A combinação de informações coletadas pela neurociência pode ajudar a prever alguns comportamentos e impulsionar vendas",[170] fomentando práticas de manipulação comportamental de consumidores por parte das empresas que se utilizam da Neurociência e do *neuromarketing*. "O Google, por exemplo, testou diferentes tons de azul na ferramenta de pesquisa para descobrir o que proporcionaria mais cliques do que os outros",[171] o que conjugou técnicas não apenas da Neurociência, como também da captologia, visto almejar a captura da atenção dos seus usuários.

Os testes de neuromarketing são feitos por meio de experimentos que envolvem **técnicas de pesquisas invasivas do ponto de vista psicojurídico** (para conferir as repercussões jurídicas, vide capítulo 5)**.** Isso porque correlacionam estímulos que conduzem a respostas inconscientes, que podem repercutir futuramente a uma manipulação dos indivíduos.

Segundo Monica Bercea, neurocientista da Universidade de Iaşi, na Romênia, as pesquisas de *neuromarketing* utilizam-se de diferentes métodos para a constatação das funções cerebral, ocular, facial, cardíaca,[172] dentre outras que corroboram para o aprimoramento da arquitetura de interfaces de plataformas e dispositivos tecnológicos. Para, portanto, adentrar os mais íntimos processos fisiológicos dos seus usuários e, com isso, saber como manipular as suas emoções e processos decisórios de uma maneira mais eficiente, plataformas digitais e *big techs* passaram a se basear nos estudos de *neuromarketing* para influenciar consciências, bem como para estimular reações inconscientes de consumo, com a finalidade de elevar sua lucratividade.

A fim de delinear como se dão esses estudos na área de *neuromarketing*, a seguir, serão apresentados os principais métodos mapeados por Bercea, bem como seus objetivos de examinação e finalidades econômicas:

---

[169] VASCONCELOS, Beatriz et al. *Neurocientistas defendem limites legais para neuromarketing:* Temor é que a estratégia possa ser usada para manipular o consumidor, publicado em 24 nov. 2021. Disponível em: <https://www1.folha.uol.com.br/especial/2021/11/neurocientistas-defendem-limites-legais-para-neuromarketing.shtml>. Acesso em 23 nov. 2022.

[170] *Idem.*

[171] *Idem.*

[172] BERCEA, Monica D. *Anatomy of methodologies for measuring consumer behavior in neuromarketing research*, 2012.

Tabela 1 – Técnicas de *neuromarketing* para análise do comportamento dos consumidores[173]

Método	Objetivo de examinação	Finalidade econômica
Imagem por Ressonância Magnética Funcional	Mapear zonas de ativação cerebral através da medição de níveis de fluxo sanguíneo e oxigenação	Constatar alterações causadas por estímulos associados às emoções inconscientes. É usada para: ● Testar novos produtos, campanhas publicitárias, preços, mudança de marcas; ● Prever comportamentos de consumidores.

[173] Os estudos de referência foram traduzidos e adaptados para a tabela de: BERCEA. *Op. cit*., 2012; VASCONSCELOS. *Op.cit*., 2021; WANG, Ying J.; MINOR, Michael S. *Validity, Reliability and Applicability of Psychophysiolgical Techniques in Marketing Research*, Psychology & Marketing, v. 25, n. 2, 2008, pp. 197-232; PLASSMANN, Hilke; RAMSØY, Thomas Z., MILOSAVLJEVIC, Milica. Faculty and Research Working Paper: Branding the Brain: A Critical Review. *INSEAD The Business School of the World*, n. 15/MKT, 2011.

Tomografia de Emissão de Pósitrons	Registrar radiação emitida de pósitrons de substância administrada no sangue	Captar sinais de percepções sensoriais e emoções. Exame utilizado com fins de: ● Testar novos produtos, anúncios publicitários e design de embalagens.
Eletroencefalograma	Registrar a atividade elétrica do cérebro por meio de eletrodos	Obter dados relacionados a mecanismos emocionais envolvidos nos processos de concentração, motivação e tomada de decisão. É utilizado para: ● Testar novos anúncios publicitários, trailers de filmes, design de websites e slogans.
Magnetoencefalografia	Averiguar campos magnéticos da atividade cerebral, na área do couro cabeludo, sem	Medir a percepção, atenção e memória a partir da avaliação de respostas cognitivas e

	dependência de outros tipos de tecido (como sangue, ossos, tecido cerebral)	afetivas, que repercutem em alterações no fluxo de fluidos cerebrais. Usualmente utilizada para: ● Testar novos anúncios publicitários, produtos e design de embalagens.
Estimulação Magnética Transcraniana	Modular atividade de certas áreas do cérebro, a partir de estimulação magnética, localizadas entre 1 e 2 centímetros em seu interior (sem atingir o neocórtex)	Inferir dados relativos à atenção, cognição e mudanças de comportamento ou respostas psicológicas mediante manipulação da atividade cerebral. É utilizada com a finalidade de: ● Testar novos produtos, anúncios publicitários e design de embalagens.
Topografia de Estado Estável		

	Registrar a atividade cerebral mediante apresentação periférica de cintilação visual sinusoidal, provocando resposta elétrica oscilatória no cérebro	Averiguar comportamento do consumidor, relativo à sua codificação de memória a longo prazo, engajamento, intensidade emocional, atenção, bem como ao seu processamento visual e olfativo. É usada para: ● Testar novos anúncios publicitários, trailers de filmes e comunicação de marcas.
Rastreamento Ocular	Medir a fixação do olhar, movimento suave de procura, dilação da pupila e piscadas	Entender comportamento do consumidor em relação à sua atenção, engajamento e memória. É usado para: ● Testar novas interfaces de sites, reações de compra, materiais de publicidade, alocação de produtos (sob o aspecto visual);

		● Analisar como consumidor filtra informações; ● Determinar hierarquia de percepção a estímulos materiais (quais elementos são percebidos ou não).
Eletromiografia Facial	Detectar os mais sutis movimentos do rosto, incluindo expressões faciais geradas a partir de estímulos visuais, táteis, gustativos e olfativos	Indicar emoções específicas em resposta a estímulos. Técnica empregada para: ● Testar reação do consumidor a publicidade (incluindo vídeos) e a *recall* de produtos.
Medição da Salivação	Relacionar essa resposta fisiológica a estímulos visuais	Parametrizar indicador do apelo apetitivo de um produto. Utilizada para:

		• Testar anúncios publicitários e design de websites; • Verificar comportamento do consumidor em seu ambiente de costume; • Averiguar reações em lojas.
Eletrocardiograma	Registrar os batimentos cardíacos e suas alterações mediante estímulos	Correlacionar alterações a respostas emocionais de estresse e tensão ou de bem-estar e tranquilidade. Técnica aplicada com objetivo de: • Testar anúncios publicitários, trailers de filmes e design de websites; • Verificar comportamento do consumidor em seu ambiente de costume.

Resposta da condutividade da pele	Avaliar a sudorese	Correlacionar a sudorese com intensidade da excitação cognitiva do indivíduo conforme provocações emocionais, pensamentos e processos de atenção. É utilizada para: ● Prever performance do mercado.

Percebe-se, pela análise da tabela, a existência de métodos mais invasivos – a exemplo da Tomografia de Emissão de Pósitrons e da Imagem por Ressonância Magnética Funcional –, que possuem a capacidade medir a atividade metabólica do cérebro; bem como de métodos menos intrusivos: que registram a atividade elétrica cerebral – e.g. Eletroencefalograma e Estimulação Magnética Transcraniana – e que não a constatam – e.g. Resposta da condutividade da pele e Rastreamento Ocular.

Diante do emprego de tais técnicas para modulação e aprimoramento de práticas manipulatórias contra consumidores, subjugando-os não apenas aos próprios experimentos, mas também à possibilidade de persuasão à aplicabilidade da manipulação em si, diversos estudiosos questionam a eticidade dessas pesquisas e da sua utilização para a finalidade a que se propõe.

Afinal, como bem pontua a professora Ana Frazão,

> (...) por mais que muitas companhias invistam hoje na neurotecnologia com nobres propósitos, como os de permitir que pacientes paralíticos possam controlar equipamentos com seus cérebros, os riscos de abusos são também muito grandes, ainda mais se os dados cerebrais passarem a ser usados para fins de manipulação da opinião e da própria personalidade das pessoas, com objetivos econômicos, políticos, religiosos, dentre outros. Assim, se já é impensável o avanço da tecnologia em qualquer seara sem o imprescindível debate ético, nesse assunto particular a reflexão ética torna-se ainda mais premente.[174]

Além dos debates éticos, os quais não são o foco deste trabalho, podemos ressaltar controvérsias relativas à privacidade, proteção de dados, bem como ao direito do consumidor e de esteio constitucional que estão sendo praticadas pelas empresas que fazem uso de tecnologias violadoras de sentimentos e processos cognitivos de tomada de decisão.

Passemos, portanto, a analisar juridicamente a violação de consentimentos dos titulares de dados pessoais submetidos a tais práticas sub-reptícias.

---

[174] FRAZÃO, Ana. *'Neurocapitalismo' e o negócio de dados cerebrais:* Os nossos pensamentos e a nossa identidade pessoal estão em risco? Publicado em: 25 set. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/neurocapitalismo-e-o-negocio-de-dados-cerebrais-25092019>. Acesso em 24 nov. 2022.

SEÇÃO II – A VIOLAÇÃO DE CONSENTIMENTOS

> *"Quando as tecnologias desse mundo mudam, somos confrontados com uma escolha. Podemos permitir que a [ideia de] eficiência governe este novo espaço, permitindo que as liberdades protegidas pela imperfeição se esvaziem; ou podemos recriar esferas de liberdade para substituir as criadas por imperfeições da tecnologia. Estas são nossas escolhas democráticas, e são escolhas reais."*
>
> LAWRENCE LESSIG[175]

Lawrence Lessig expõe, em sua obra *Reading The Constitution in Cyberspace*, que uma sociedade democrática, ao se deparar diante de inovações tecnológicas, pode se submeter passivamente aos riscos que essas inovações trazem aos direitos fundamentais dos cidadãos ou pode ampliar os próprios direitos fundamentais dos cidadãos como uma maneira de se adaptar às disrupções tecnocientíficas.

Por muito tempo, os cidadãos brasileiros viram-se – e ainda têm-se visto – submetidos a práticas abusivas por parte de empresas privadas e agentes do Estado que fazem uso da tecnologia para se beneficiar da coleta e do tratamento ilícito de seus dados pessoais, com fins estritamente lucrativos.

Foi assim que o Estado brasileiro viu-se diante da controvérsia de Lessig: submeter os cidadãos aos perigos da tecnologia ou ampliar os direitos fundamentais da Constituição Federal para se adaptar às inovações do advento tecnológico? Assim, foi criado o direito fundamental à proteção de dados pessoais pela Emenda Constitucional nº 115 (vide capítulo 4), em uma diligência a favor do alargamento do rol de salvaguardas aos cidadãos.

Logo, diante do cenário relatado na seção I deste trabalho, torna-se de suma importância delinear as repercussões jurídicas do emprego de técnicas manipulatórias contra titulares de

[175] Tradução livre: "When the technologies of that world change, we confront a choice. We could imagine allowing efficiency to rule this new space, by allowing liberties protected by imperfection to fall away; or we could imagine recreating spheres of liberty to replace those created by imperfections in technology. These are our democratic choices, and real choices they are." – LESSIG, Lawrence. *Reading The Constitution in Cyberspace*. Emory Law Review, v. 45, 1996, p. 43.

dados por parte do setor privado da economia capitalista datificada, principalmente no que concerne às violações à principal expressão da sua capacidade volitiva: o consentimento.

Para o campo da proteção de dados, o consentimento é o instrumento que representa a manifestação individual na seara dos direitos da personalidade,[176] por essa razão, promove a própria personalidade de um indivíduo. Possui, desse modo, intrínseca relação com a construção da sua esfera privada e sua "autodeterminação existencial e informacional."[177] Bem como se mostra essencial para a proteção do titular e para a circulação da informação[178] no capitalismo de vigilância datificado.

Portanto, nesta seção, abordaremos o arcabouço normativo que confere salvaguardas e direitos aos titulares de dados; assim como, diante disso, quais são as principais violações decorrentes das práticas sub-reptícias relatadas na seção I. Ademais, serão propostos mecanismos regulatórios e meios de contravigilância por parte do cidadão, de modo a reforçar as garantias constitucionais e legislativas dos titulares em detrimento dos riscos advindos da economia caracterizada pela extração ilícita de dados.

O principal escopo desta seção II é propor uma série de medidas concretas para que a arquitetura de vigilância característica desta **economia "danificada" pela obtenção sub-reptícia de dados** pessoais seja, ao menos em certa medida, convertida em um **sistema datificado** pautado pela **observância das estruturas democráticas** contidas na Constituição Federal.

Para isso, antes de mais nada, analisaremos o conjunto de normas que garante a proteção e as salvaguardas aos titulares de dados no ordenamento jurídico brasileiro, para posteriormente elucidarmos as violações que ocorrem constantemente na sociedade de vigilância e como dirimi-las diante dos mecanismos de que dispomos.

[176] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 120.
[177] *Idem.*
[178] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 377.

CAPÍTULO 4 – O arcabouço jurídico de proteção aos titulares de dados

As normas relativas aos direitos dos titulares de dados pessoais podem ser encontradas em diferentes dispositivos normativos do ordenamento jurídico brasileiro. Quando nos referimos a titular de dados, podemos versar a respeito de situações que envolvem a Lei Geral de Proteção de Dados (LGPD), o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet (MCI).

Contudo, para que adentremos especificamente em cada um deles, antes devemos perpassar o entendimento de um direito novo, porém extremamente importante e que, por essa razão, merece destaque neste capítulo: o direito à proteção de dados pessoais. A partir de sua compreensão, torna-se possível estabelecer tanto a relevância da "dimensão digital dos direitos fundamentais"[179] dos titulares, quanto as repercussões que essa dimensão tem nas outras searas, como no direito à privacidade, à personalidade e no direito consumerista.

4.1 – O direito fundamental à proteção de dados pessoais: breve panorama histórico, desvinculação do direito à privacidade e dupla função vinculante

No dia 10 de fevereiro de 2022, foi promulgada a Emenda Constitucional (EC) nº 115, que acrescentou aos incisos do artigo 5º da Constituição Federal (CF) o inciso LXXIX, cuja redação dispõe que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".[180] Adicionalmente, designou como competência da União a organização e fiscalização da proteção e tratamento de dados pessoais (art. 21, XXVI, CF), bem como a legislação relativa à matéria sobre proteção de dados (art. 22, XXX, CF).

Para que os cidadãos brasileiros tenham alcançado tamanha conquista em âmbito constitucional para segurança jurídica da garantia de direitos oponíveis[181] contra situações abusivas por parte daqueles que porventura façam uso ilícito de seus dados pessoais – bem como na seara regulatória com a criação da Autoridade Nacional de Proteção de Dados

[179] As palavras são de: SARLET, Ingo Wolfgang. Fundamentos Constitucionais: O direito fundamental à proteção de dados. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 22.

[180] BRASIL. *Constituição da República Federativa do Brasil de 1988*, Brasília, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 04 dez. 2022.

[181] A referência é de Ronald Dworkin, cuja visão dos direitos fundamentais consistia em uma consubstancialização de posições jurídicas dos cidadãos oponíveis contra o Estado, de maneira a denominá-los de "trunfos contra a maioria". – DWORKIN, Ronald. *Levando os direitos a sério*, São Paulo: Martins Fontes, 2002.

(ANPD)[182] –, torna-se importante ressaltar que o caminho percorrido foi longo e influenciado por experiências externas. Logo, a fim de que possamos entender como o ordenamento jurídico brasileiro incorporou a noção de proteção de dados pessoais, que foi posteriormente consubstanciada em direito fundamental pela EC nº 115, cabe realizar primeiramente um aparato histórico das principais influências que repercutiram diretamente no cenário pátrio.

A concepção brasileira atual de proteção de dados é fortemente ligada a marcos regulatórios europeus e a institutos jurídicos estadunidenses, tendo em vista que, em ambas localidades, o desenvolvimento tecnocientífico se deu de maneira anterior e mais intensa se comparada à do Brasil. A relação entre os processos originários do direito à proteção de dados é bem pontuada por Danilo Doneda, ao enfatizar que:

> Alguns dos institutos fundamentais de proteção de dados, hoje fortemente entrincheirados na Lei Geral de Proteção de Dados brasileira (LGPD) como no Regulamento Geral de Proteção de Dados europeu (GDPR) e em tantas outras, remontam, em última análise, a formulações regulatórias que tiveram lugar nos Estados Unidos. Nesse país, uma parcela considerável do conteúdo presente nos atuais marcos regulatórios sobre a matéria foi originariamente concebida, bem como tiveram lugar alguns dos primeiros e mais importantes debates sobre o tema.[183]

Diante disso, cabe ressaltar que uma importante influência para a proteção de dados adveio do direito estadunidense, especificamente do **artigo *The Right to Privacy***, de Samuel Warren e Louis Brandeis, que, em 1890, passou a enunciar o "direito a ser deixado só"[184] (***the right to be left alone***). Tal compreensão da privacidade foi um marco importante futuramente para o campo da proteção de dados devido à hermenêutica conferida entre a relação da tutela da privacidade e o progresso tecnológico, apesar de ainda constituir uma noção individualista e isolacionista.[185]

Todavia, o primeiro diploma normativo que abordou especificamente o tema da proteção de dados pessoais foi a **Lei de Proteção de Dados do *Land* Alemão de Hesse**, na década de 1970. Por utilizar-se pela primeira vez do vocábulo *Datenshutz* – proteção de dados

---

[182] A Autoridade Nacional de Proteção de Dados é atualmente uma autarquia federal responsável por "proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural", bem como o relativo à proteção de dados pessoais. – *Cf.*: ANPD. Autoridade Nacional de Proteção de Dados, *Portaria nº 1, de 08 de março de 2021*. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618>. Acesso em 10. dez. 2022.

[183] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 5.

[184] Tradução livre de: WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*, Harvard Law Review, 4/5, 1890, pp. 193-200.

[185] SARLET. *Op. cit.*, 2023, p. 32.

–, em vez dos referentes à segurança da informação,[186] como normalmente se fazia à época, contribuiu para uma "mudança de perspectiva concreta"[187] em relação ao direito à proteção de dados pessoais como direito autônomo ao da privacidade e da segurança da informação.

Ademais, vale mencionar o **relatório do Departamento de Saúde, Educação e Bem-Estar (HEW)**[188], de 1973, intitulado *Records, Computers and the Rights of Citizens*: *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*[189], cuja proposição dos chamados ***Fair Information Practice Principles*** gerou grande influência nos parâmetros adotados pelo marco regulatório brasileiro ao estabelecer os princípios da finalidade, transparência, adequação, qualidade, correção e segurança[190] como alguns dos norteadores da Lei Geral de Proteção de Dados.

Por fim, o último marco histórico relevante a ser trazido é a **decisão do Tribunal Constitucional Alemão de 1983**, que, ao analisar a constitucionalidade da Lei do Censo de 1982, reconheceu a existência de riscos às garantias e direitos dos titulares de dados que iam muito além dos relativos à privacidade, tendo em vista a possibilidade do processamento de um enorme volume de dados diante do avanço tecnológico, bem como a relevância dos próprios dados pessoais.[191] Nesse sentido, ao prezar pela importância de cada dado pessoal, o Tribunal averiguou a existência do **direito à autodeterminação informativa** do titular, "formulado a partir do direito geral de personalidade e voltado a garantir ao cidadão o direito de controlar a amplitude da divulgação ou utilização"[192] de seus dados.

Vale lembrar, todavia, que a autodeterminação informativa não constitui um direito absoluto do titular, ou seja, não significa um controle incondicional do titular sobre os seus dados, considerando que podem sofrer restrições de tratamentos que "seriam justificados em

---

[186] *Datensicherung* e *Datensicherheit* eram os termos usualmente utilizados para referir-se à segurança da informação – *Cf.*: *Ibid*., p. 8.
[187] *Idem.*
[188] Em inglês, Department of Health, Education and Welfare (HEW).
[189] ESTADOS UNIDOS. U.S Department of Health, Education and Welfare (HEW). *Records, Computers and the Rights of Citizens*: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Library Department of Justice, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 29 nov. 2022.
[190] DONEDA. *Op. cit*., 2023, p. 7.
[191] Nos termos do Tribunal Constitucional Alemão no julgamento da Lei do Censo de 1983, "não existem mais dados insignificantes no contexto do processamento eletrônico de dados*"*. – BVerfGE 65, 1, "Recenseamento" (Volkszählung). MARTINS, Leonardo. (org.) *Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005, pp. 244-245.
[192] DONEDA. *Op. cit*., 2023, p. 9.

nome de um interesse geral preponderante".[193] Porém, de acordo com Hans-Peter Bull, o que teria baseado a decisão do Tribunal Constitucional Alemão ao reconhecer tal direito seria assegurar aos cidadãos justamente a sua liberdade em face da repressão estatal, devendo ser a transparência a regra da Administração Pública para a persecução das suas finalidades.[194]

Diante disso, foi estabelecido um vínculo entre autodeterminação informativa, privacidade e proteção de dados, na medida em que a primeira se manifesta em **uma noção negativa e positiva** no que concerne ao livre desenvolvimento da personalidade de um indivíduo e à sua tomada de decisão referente aos seus direitos personalíssimos. Quanto a isso, cabe então **distinguir privacidade de proteção de dados pessoais**.

Para Stefano Rodotà, a privacidade indicaria uma concepção negativa e estática que impossibilitaria a interferência de terceiros nos direitos de personalidade de um indivíduo.[195] Essa perspectiva coaduna-se com a ideia da **teoria das três esferas de proteção da personalidade**,[196] que subdivide a privacidade em três níveis imutáveis de garantias: i) íntima; ii) privada ou individual; e iii) social ou pública. Essa teoria foi amplamente criticada, tendo destaque o argumento de Spiros Simitis, que expõe haver uma insuficiência na moldura estática proposta para a resolução dos problemas advindos da inter-relação e sobreposição prática das esferas.[197]

Essa insuficiência, em contrapartida, seria suprida, em certa medida, pela proteção de dados pessoais, visto conferir ao titular, ainda de acordo com Rodotà, um conjunto de poderes positivos e dinâmicos.[198] A partir da capacidade de controle sobre a coleta e o tratamento dos dados que o identifiquem ou possam o identificar, foi concedido ao titular de dados uma dinamicidade da moldura de inter-relações das previamente denominadas esferas de proteção da personalidade.

---

[193] MENDES, Laura Schertel. *Habeas data e autodeterminação informativa*: dois lados da mesma moeda, Direitos Fundamentais & Justiça, Belo Horizonte, v. 12, n. 39, pp. 185-216, 2018, p. 188.
[194] Quanto à interpretação de Bull, vide: BULL, Hans-Peter. *Informationelle Selbstbestimmung*: Vision oder Illusion?, Tübinger:Mohr Siebeck, 2009, p. 29 e ss.
[195] RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 17.
[196] A teoria das três esferas de proteção da personalidade, também denominada de "teoria dos círculos concêntricos", foi cunhada por Heinrich Hubmann e Heinrich Henkel na Alemanha, na década de 1950, para se referir ao sistema jurídico de tutela da privacidade, em que estariam abarcados o *privatsphare* (direito à privacidade *stricto sensu*), o *vertrauenssphare* (direito à intimidade) e o *geheimphare* ou *vertraulichkeitssphare* (direito ao segredo). – Vide: COSTA JR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: RT, 1995.
[197] SARLET. *Op. cit.*, 2023, p. 32.
[198] RODOTÀ. Op. cit., 2008, p. 17.

Com isso, Rodotà expõe que a principal diferença entre privacidade e proteção de dados residiria no **bem jurídico tutelado** por cada um desses direitos: enquanto a **privacidade** tutelaria a **informação e o sigilo – em uma lógica binária de restrição** –; a **proteção de dados** abarcaria a **circulação e o controle da informação – em um sentido de adequação do fluxo informacional.**[199]

Bruno Bioni ainda alerta que a ideia de que o direito à proteção de dados é uma mera evolução do direito à privacidade constitui uma "construção dogmática falha".[200] Isso porque o próprio objeto do direito à proteção de dados é muito mais amplo do que o à privacidade, abrangendo todos os dados relativos a uma pessoa determinada ou determinável – **sendo insignificante o pertencimento a alguma das esferas[201] de proteção à personalidade para sua aplicação**.

Logo, considerando a delineação histórica feita até aqui e partindo da compreensão do bem jurídico tutelado por este direito, a proteção de dados cumpre uma dupla função, como bem expõe Bruno Bioni, "de não só garantir a privacidade e outros direitos fundamentais, mas também [de] fomentar o desenvolvimento econômico".[202]

A partir do momento em que o legislador brasileiro viu-se diante do desafio de conciliar a garantia de direitos fundamentais de titulares e o livre desenvolvimento econômico, tornou-se de suma importância a criação de uma Lei Geral de Proteção de Dados que pudesse parametrizar as regras que pudessem ser aplicadas aos casos concretos, a fim de que pudesse ser dada eficácia à dupla função da proteção de dados pessoais.

Assim, após um processo que tramitou por cerca de oito anos – percorrendo o Ministério da Justiça, a Casa Civil da Presidência da República, a Câmara dos Deputados e o Senado Federal[203] –, foi promulgada em 2018 a Lei Geral de Proteção de Dados (LGPD) brasileira, cujos principais aspectos passaremos a discorrer a seguir.

---

[199] *Ibid*., p. 36.
[200] BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento, 3ª ed., Rio de Janeiro: Forense, 2021, p. 95.
[201] SARLET. *Op. cit.*, 2023, p. 33.
[202] BIONI. *Op. cit*., 2021, p. 108.
[203] DONEDA. *Op. cit.*, 2023, pp. 16-17.

4.2 – A Lei Geral de Proteção de Dados: princípios norteadores, bases legais e dados pessoais (sensíveis e não sensíveis)

A Lei nº 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados, incorporou ao ordenamento jurídico brasileiro, como visto no subcapítulo anterior, princípios e valores da seara da proteção de dados pessoais baseados em experiências prévias da Europa e dos Estados Unidos e adaptados ao contexto pátrio.

Por exemplo, a autodeterminação informativa, direito cunhado pelo Tribunal Constitucional Alemão ao analisar a constitucionalidade da Lei do Censo de 1982, está preconizada na LGPD em seu artigo 2º, inciso II, como um de seus principais fundamentos; bem como a privacidade, a liberdade de informação e de comunicação, a inviolabilidade da honra e da imagem, e o desenvolvimento econômico.[204]

Dessa feita, pode-se notar que a LGPD acompanha as propostas internacionais de normas de proteção de dados cujo objetivo não se restringe a garantir a tutela de direitos aos titulares, mas também a promover o crescimento tecnocientífico e garantir a livre concorrência e iniciativa. Essa dupla função,[205] contudo, não exime as responsabilidades de salvaguardas aos titulares de dados pessoais cujas informações são processadas por agentes de tratamento[206] diariamente no capitalismo de vigilância datificado.

Controladores e operadores possuem deveres de observância a princípios e hipóteses contidos na própria Lei Geral de Proteção de Dados que, se não respeitados, deslegitimam o seu tratamento. Primeiramente discorreremos a respeito dos princípios preconizados pela

---

[204] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a **liberdade** de expressão, **de informação, de comunicação** e de opinião;
IV - a **inviolabilidade da** intimidade, **da honra e da imagem**;
V - o **desenvolvimento econômico** e tecnológico e a inovação;
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (grifos nossos) – BRASIL, *Lei nº 13.709, de 14 ago. 2018*, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 05 dez. 2022.

[205] BIONI. *Op. cit*., 2021, p. 108.

[206] Para os fins da LGPD, agentes de tratamento são controlados e operadores de dados (vide art. 5º, IX). Sendo controlador a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI) e operador "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII) – BRASIL, *Op. cit*., 2018.

referida lei para, em seguida, passaremos a abordar os requisitos de tratamento, isto é, as bases legais que legitimam o processamento dos dados pessoais[207] pelos agentes.

A LGPD elenca, ao todo, dez princípios que devem nortear todo tratamento de dados pessoais realizado em âmbito nacional, sendo todos eles alicerçados **no princípio basilar da boa-fé** – contido no *caput* do artigo 6º da lei, indicando sua centralidade na comunhão principiológica, podendo ser considerado "**o princípio dos princípios**".[208] Os demais princípios, otimizados pela boa-fé,[209] estão elencados no artigo 6º da LGPD na seguinte ordem:

1. **Finalidade**: este princípio estabelece que os propósitos do tratamento devem, ser legítimos, especificados e informados explicitamente ao titular, devendo quaisquer processamentos ulteriores, isto é, qualquer uso secundário dos dados originalmente coletados, serem compatíveis com as finalidades originárias.

2. **Adequação**: por sua vez, este princípio indica a necessidade de haver compatibilidade do tratamento com as finalidades informadas – novamente, de maneira legítima, específica e explícita – ao titular, sempre de acordo com o contexto do tratamento. A compatibilidade do tratamento, por ser um conceito jurídico indeterminado,[210] trata-se de um exercício hermenêutico do intérprete a partir da conjugação principiológica entre adequação, finalidade e boa-fé.

3. **Necessidade**: relacionado à noção de minimização, limita o tratamento ao mínimo necessário para a realização das finalidades propostas no momento da coleta dos dados pessoais, ao abranger apenas aqueles pertinentes, proporcionais e não excessivos relativos à persecução dos objetivos do processamento.

4. **Livre acesso**: garante ao titular a consulta facilitada e gratuita em relação à forma e duração do tratamento, assim como sobre a integralidade dos seus dados pessoais que

[207] Importa ressaltar que dado pessoal, para a LGPD, é toda "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I), não abarcando, portanto, aquele anonimizado. – *Idem*.
[208] BIONI, Bruno Ricardo; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD:* quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021, p. 23. Disponível em: <https://www.observatorioprivacidade.com.br/2021/01/29/legitimo-interesse-na-lgpd-quadro-geral-e-exemplos-de-aplicacao/>. Acesso em 05 dez. 2022.
[209] Insta salientar ainda que o princípio da boa-fé, em sua condição objetiva, veda o abuso de direitos na realização de quaisquer atividades de tratamento de dados, os quais devem sempre observar padrões sociais, morais e éticos. Vide: *Ibid.*, p. 30.
[210] Antonio Menezes Cordeiro refere-se a uma busca metajurídica do intérprete ao tentar definir conceitos de demasiada elasticidade. Vide: MENEZES CORDEIRO, Antonio Manuel da Rocha e. *Da boa-fé no Direito Civil*, Coimbra: Almedina, 2011, p. 1121.

estão sob processamento do agente. Este princípio tem especial relevância no que tange à portabilidade e interoperabilidade de seus dados pessoais, nos termos do artigo 40 da LGPD.

5. **Qualidade dos dados**: garante ao titular a clareza, exatidão, relevância e atualização de seus dados pessoais, de acordo com a necessidade e a fim de cumprir a finalidade do tratamento. Possui intrínseca relação com a transparência, visto ser essencial para a concretização de uma comunicação clara, precisa e facilmente acessível.

6. **Transparência**: assegura ao titular informações claras e precisas, bem como facilmente acessíveis, sobre a realização do tratamento de seus dados e os respectivos agentes que os processam – observados os segredos comercial e industrial. Os artigos 8º, §6º; 9º; 14, §2º; e 7º da LGPD, ao depositarem nos controladores a obrigação de fornecerem informações para os titulares de dados sobre as atividades de tratamento de dados pessoais, indicam a necessidade de se garantir a transparência do fluxo informacional.

7. **Segurança**: este princípio prevê a utilização de medidas técnicas e administrativas capazes de proteger os dados pessoais do titular contra incidentes de segurança e vazamento de dados – acessos não autorizados (comprometendo sua confidencialidade) e situações acidentais ou ilícitas de destruição, perda, alteração (violando sua integridade), comunicação ou difusão.

8. **Prevenção**: garante a adoção de medidas preventivas contra a ocorrência de danos decorrentes do tratamento de dados pessoais. A própria implementação de medidas de segurança, abordadas anteriormente, quando adotadas desde a concepção do produto ou serviço (*privacy by design*), em detrimento de uma posição reativa, é um exemplo de aplicação do princípio da prevenção (arts. 46 a 49, LGPD).

9. **Não discriminação**: este princípio veda a realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos. Em alusão ao que foi abordado na seção I deste trabalho, a LGPD proíbe, portanto, os casos de *profiling* discriminatórios exemplificados por Cathy O'Neil em *Weapons of math destruction*,[211] bem como o

[211] O'NEIL. *Op. cit.,* 2016.

monitoramento de grupos socialmente vulnerabilizados, que repercute em um *feedback looping* de injustiça, nos termos de Virginia Eubanks.[212]

10. **Responsabilização e prestação de contas (ou *accountability*)**:[213] assegura a demonstração, pelo agente de tratamento, da adoção de medidas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, assim como da eficácia das medidas adotadas. O termo *accountability*, segundo Bruno Bioni, é um conceito cuja "polissemia"[214] gera um debate conceitual no campo das ciências sociais até os dias atuais; entretanto, neste contexto, pode ser definido como o princípio que possibilita uma auditoria das medidas de salvaguardas adotadas pelos agentes de tratamento por parte dos titulares em relação aos seus dados pessoais.

Diante de sua base principiológica, a LGPD define parâmetros de boas práticas para o tratamento de dados pessoais que controladores e operadores devem observar durante todo o ciclo de vida dos dados – desde sua coleta até sua eliminação e descarte. Todavia, além de princípios norteadores, a lei enuncia bases legais que legitimam o tratamento e que conferem-no requisitos de validade, podendo ser utilizadas em concomitância dependendo da situação concreta.[215]

Essas hipóteses estão previstas nos seus artigos 7º e 11, respectivamente no que diz respeito ao tratamento de dados pessoais não sensíveis e sensíveis.[216] Ao todo – e **sem distinção**

[212] EUBANKS. *Op. cit*., 2018.
[213] Todas as conceituações dos princípios foram baseadas na própria LGPD (Art. 6º, incisos I a X). *Cf.*: BRASIL, *Op. cit*., 2018.
[214] "Um conceito guarda-chuva, de ouro, multiforme ou camaleão. É dessa forma que a literatura, principalmente do campo das ciências sociais, refere-se à *accountability*, por ser um termo bastante elusivo ao qual se pode atribuir os mais diferentes significados. Responsabilidade, equidade, integridade, eficiência, eficácia, transparência e, até mesmo, democracia são apenas alguns deles. Essa polissemia, além de dificultar o trabalho dos tradutores que optam frequente- mente por utilizar o termo em inglês em vez de versá-lo em outra língua, não passa ou não deveria passar despercebida também pelos juristas." – BIONI, Bruno Ricardo. *Regulação e proteção de dados pessoais*: o princípio da accountability, 1ª Ed.,Rio de Janeiro: Forense, 2022, p. 21.
[215] "Entende-se que, ainda que seja possível utilizar mais de uma base legal para determinado tratamento de dados, é preciso buscar a base mais *adequada* e *segura* para a situação concreta. – VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 131.
[216] Segundo o artigo 5º, inciso II, da LGPD, dados sensíveis são aqueles dados pessoais que referem-se sobre a origem étnica ou racial, convicção religiosa, opinião política ou filiação a sindicato ou organização de caráter religioso, filosófico ou político; bem como aqueles que versem sobre saúde ou vida sexual e dados genéticos ou biométricos. – BRASIL, *Op. cit*., 2018.

de nível hierárquico[217] – são enumeradas **dez bases legais** que possibilitam o tratamento de **dados pessoais não sensíveis** pelo artigo 7º da LGPD, sendo elas:

1. **Consentimento**: mediante esta base legal, que será melhor elucidada no subcapítulo 4.3, o titular tem o direito à manifestação volitiva de sua tomada de decisão "livre, informada e inequívoca"[218] para que os agentes de tratamento se utilizem dos seus dados pessoais de acordo com as finalidades determinadas. Por ora, cabe pontuar que o consentimento pode ser revogado[219] a qualquer momento pelo titular mediante manifestação expressa, de acordo com o artigo 8º, §5º, da LGPD.

2**. Cumprimento de obrigação legal ou regulatória pelo controlador**: esta base legal pode ser bem delineada por políticas de privacidade e tratamento de dados que estabeleçam claramente a necessidade de cumprimento das obrigações contratuais e regulatórias por parte de empresas da área de seguro, de saúde suplementar ou do mercado financeiro, as quais estão submetidas a diversas regras legais e regulatórias.[220]

3. **Tratamento e uso compartilhado, pela Administração Pública, de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres**: trata-se da previsão do processamento de dados pessoais pelo poder público, observadas as disposições do Capítulo IV e do artigo 23[221] da LGPD, o qual se refere ao tratamento de dados pelas pessoas jurídicas de direito público citadas pela Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) – em seu artigo 1º, §único.[222] As políticas públicas em

[217] BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 161.

[218] O artigo 5º, inciso XII, da LGPD define consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; – *Idem*.

[219] Trata-se, segundo Bruno Bioni, de um direito potestativo a partir do momento que "confere ao titular a possibilidade de constituir, modificar ou extinguir uma situação subjetiva com uma declaração de vontade, sem que a outra parte possa se opor." – BIONI. Op. cit. 2023, p. 171. (nota de rodapé 41)

[220] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 131.

[221] O artigo 23 ainda define que a Administração Pública deve realizar o tratamento de dados pessoais com fins de atender **finalidades públicas**, na persecução de **interesses públicos** e com o objetivo de executar competências legais ou cumprir atribuições legais do serviço público, desde que: "sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e 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;" e "III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei". – BRASIL, *Op. cit*., 2018.

[222] "Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

questão podem envolver, por exemplo, "a implementação de saneamento básico, de auxílios a cidadãos em situações de vulnerabilidade ou de projetos voltados à educação".[223]

4. **Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais**: esta base legal introduz o conceito contido no artigo 5º, inciso XVIII, da LGPD, que define órgão de pesquisa como "órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico".[224] É este, na roupagem de controlador, o responsável em pesquisas por tratar dados pessoais, cuja recomendação é a de serem anonimizados, em razão de a Lei entender ser esta uma medida protetiva para os titulares. Assim, as instituições de pesquisa tornam-se responsáveis pela segurança dos dados tratados, devendo considerar os padrões éticos relacionados aos estudos, bem como à divulgação de seus resultados – nunca podendo ser revelados os dados pessoais nesta hipótese.[225]

5. **Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados**: essa disposição permite ao agente tratar os dados pessoais do titular que são essenciais para a contratação de determinado produto ou serviço, somente sendo necessário que o titular seja "parte ou esteja em tratativas para a execução de um contrato".[226] Esta base legal difere-se do consentimento a partir do momento em que o titular não pode revogar o fornecimento de seus dados aos agentes de tratamento a qualquer momento, visto encontrarem

---

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." (grifos nossos) – BRASIL. *Lei nº 12.527, de 18 de novembro de 2011.* Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 10 dez. 2022.

[223] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 131.
[224] BRASIL, *Op. cit.*, 2018.
[225] VIOLA; TEFFÉ. *Op. cit.*, 2023, pp. 132-133.
[226] *Ibid.*, p. 133.

respaldo legal na LGPD para manter esses dados enquanto durar a execução do negócio jurídico.[227]

6. **Exercício regular de direitos em processo judicial, administrativo ou arbitral**:[228] nos casos em que os dados pessoais podem servir como fatores úteis para o exercício de direitos em demandas processuais, eles possuem a possibilidade de serem armazenados e tratados, desde que haja real necessidade e para essa específica finalidade.[229] Isso porque o uso de dados pessoais em processos – sejam eles judicias, administrativos ou arbitrais – garante o direito de produção de provas das partes, além de que esta base legal "compreende ações do cidadão comum autorizadas pela existência de direito definido em lei",[230] vedando condutas abusivas ou desempenho disfuncional de posição jurídica pelas partes.

7. **Proteção da vida ou da incolumidade física do titular ou de terceiro**: esta é uma hipótese autorizativa de tratamento em situações excepcionais, não podendo ser justificada de maneira genérica, devendo ser passível de comprovação o risco à vida ou à incolumidade física do titular ou de terceiro. Dois exemplos trazidos por Mário Viola e Chiara de Teffé que ilustram o uso desta base legal seria a obtenção de dados de geolocalização de *smartphones* para: i) localizar vítimas desaparecidas em desastres; e ii) constatar áreas de aglomeração de pessoas durante a pandemia da Covid-19.[231]

8. **Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária**: esta base legal merece especial atenção em decorrência da possibilidade da inferência de dados sensíveis de titulares a partir da solicitação de exames ou de outros dados de saúde, que, se não utilizados de maneira lícita e adequada, podem repercutir em discriminações ilícitas e abusivas.[232] O tratamento dos dados relativos à tutela da saúde pode ser realizado quando necessário para atender às finalidades legítimas almejadas por controladores ou terceiros, exceto

[227] *Ibid.*, p. 134.
[228] Neste caso, nos termos da Lei de Arbitragem (Lei nº 9.307/1996). Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9307.htm>. Acesso em 10 dez. 2022.
[229] LIMA, Caio César C. Seção I – Dos requisitos para o tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato (coord.). *LGPD – Lei Geral de Proteção de Dados*. São Paulo: RT, 2019, p. 184.
[230] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 134.
[231] *Ibid.*, p. 135.
[232] *Idem.*

nos casos em que – após o devido teste de balanceamento[233] – as salvaguardas e os direitos fundamentais de proteção de dados dos titulares prevalecerem.

9. **Legítimo interesse**:[234] há uma certa flexibilidade e dinamicidade na aplicação desta base legal. Isso decorre devido à necessidade de se balancear as expectativas legítimas dos titulares em relação ao uso dos seus dados com os interesses legítimos dos agentes de tratamento, que devem observar os princípios da necessidade, finalidade e adequação para a persecução de suas finalidades. Tal balanceamento é realizado por meio do chamado ***legitimate interests assessment*** **(LIA)**, considerado um teste multifatorial[235] de sopesamento entre direitos de titulares de dados e agentes de tratamento, sendo dividido na verificação: i) da situação concreta e finalidade legítima do tratamento[236] (art.10, *caput* e inciso I, da LGPD); ii) da noção de minimização, a partir da coleta de dados estritamente necessários para a persecução das finalidades[237] (art. 10, § 1º); iii) do balanceamento entre impactos sobre o titular e legítimas expectativas[238] dos agentes de tratamento (art. 10, inciso II); e iv) da adoção de salvaguardas de transparência e minimização de riscos aos titulares[239] por parte dos agentes (art. 10, §§ 2º e 3º). Cabe ressaltar ainda que esta hipótese autorizativa é utilizada em situações em que a obtenção do consentimento do titular poderia atrasar ou inviabilizar o tratamento dos seus dados[240] ou quando simplesmente não houver a possibilidade de o agente se utilizar de

[233] Referimo-nos aqui ao teste de balanceamento do legítimo interesse, que será elucidado no próximo item de base legal.
[234] A definição de "legítimo interesse" está ainda sendo construída no ordenamento jurídico brasileiro, cabendo à ANPD e ao Poder Judiciário preencher essa lacuna. – BUCAR, Daniel; VIOLA, Mario. Tratamento de dados pessoais por "legítimo interesse do controlador": primeiras questões e apontamentos. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Editora Revista dos Tribunais, 2019.
[235] Nomenclatura utilizada por: BIONI. *Op. cit.*, 2023, p. 162.
[236] "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador (...)" – BRASIL. *Op. cit.*, 2018.
[237] "§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados." – *Idem*.
[238] "Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: (...)
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei." (grifos nossos) – *Idem.*
[239] "2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial." – *Idem*.
[240] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 126.

outra base legal para fundamentar a persecução de suas finalidades legítimas. Por fim, insta salientar que quando o interesse for de um terceiro à cadeia de tratamento, o legítimo interesse poderá ser aplicado em situações em que este terceiro não estiver apto a obter o consentimento do titular ou se este tipo de obtenção inviabilizar o processamento dos dados.[241]

10. **Proteção do crédito**: esta base legal procura, ao menos a princípio, ampliar e otimizar a concessão de crédito, além de melhor análise de risco por parte dos credores e impulsionar o mercado de consumo.[242] Para isso, esta hipótese autorizativa deve dialogar constantemente com o Código de Defesa do Consumidor (CDC), bem como com a Lei do Cadastro Positivo (Lei nº12.414/2011), a fim de que sejam evitadas condutas abusivas – como o tratamento de dados excessivos para análise de *credit scoring*, como será melhor discorrido no subcapítulo 4.4.

Diante do rol de hipóteses de requisitos apresentados, vale frisar que os agentes de tratamento devem priorizar a escolha de uma única base legal para justificar a utilização dos dados pessoais de titulares, "ainda que seja possível utilizar mais de uma base legal para determinado tratamento".[243]

No que concerne às **bases legais** que permitem a coleta e processamento de **dados sensíveis**, cabe pontuar que, dependendo do contexto, seu tratamento pode propiciar risco significativo para os direitos e liberdades fundamentais dos titulares, motivo pelo qual sua proteção foi pormenorizada pela LGPD de forma mais rígida – se comparada à de dados não sensíveis. Ademais, para determinar se um dado é sensível ou não, torna-se essencial verificar o **contexto de seu processamento**, bem como as r**elações que podem ser inferidas com as demais informações** disponíveis e a possibilidade de seu tratamento servir como instrumento de **estigmatização ou discriminação**.[244]

A partir da análise do artigo 11 da LGPD, que versa sobre as hipóteses de tratamento de dados sensíveis, podemos constatar a manutenção de várias das bases legais do artigo 7º – com

[241] BIONI. *Op. cit*., 2021, p. 232.
[242] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 135.
[243] *Idem*, p. 131.
[244] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Editora Revista dos Tribunais, 2019, pp. 460 e ss.

e sem o fornecimento do consentimento do titular[245] (incisos I e II do artigo 11, respectivamente). Todavia, o legislador preferiu excluir dos requisitos do artigo 11 as hipóteses de atendimento ao legítimo interesse legítimo do controlador e de terceiro, bem como a base legal de proteção ao crédito. Nos termos de Mario Viola e Chiara de Teffé,

> **No lugar da hipótese relativa ao legítimo interesse, o Art. 11, II, "g", trouxe base mais específica, que visa à prevenção de fraudes e garantir a segurança do titular,** restando vinculada aos interesses dos titulares e determinadas entidades. Como exemplo de aplicação, aponta-se a seguinte situação: **instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária por meio de um caixa eletrônico**, por exemplo. Adicionalmente, pode-se mencionar a exigência para atendimento médico-hospitalar, com a utilização de seguro ou plano de assistência à saúde, que o segurado/beneficiário coloque seu polegar em um leitor biométrico para confirmar sua identidade, a fim de evitar que outra pessoa utilize a cobertura securitária em seu lugar.
> Além disso, **a norma acrescentou a possibilidade de exercício regular de direitos também em relação a um contrato (Art. 11, II, "d"), mas não replicou a disposição do Art. 7º, V.** Nesse caso, como exemplo, recorda-se a **situação de um seguro saúde ou seguro de vida necessitar coletar informações sensíveis, com base no exercício regular de direitos, pois, sem o tratamento de tais dados, poderá não ser possível entregar a prestação que lhe compete decorrente da relação contratual**, como o ressarcimento de despesas médicas no seguro saúde ou o pagamento de indenização por algum tipo de invalidez decorrente de acidente ou doença nos seguros de pessoas. Afirma-se que, aqui, **a seguradora não teria apenas o dever de cumprir a obrigação contratual, mas também o direito de adimpli-la. Da mesma forma, a doutrina europeia tratando de dispositivo similar no GDPR reconhece a possibilidade de uma seguradora – com base no exercício regular de direitos decorrentes de um contrato – tratar dados de saúde de um segurado para verificar a regularidade de uma reclamação de indenização oriunda de um sinistro de seguros de pessoas**. (grifos nossos) [246]

Nota-se, portanto, a preocupação do legislador em garantir mecanismos de salvaguardas ao titular para melhor exercício de sua autodeterminação informativa quanto aos seus dados sensíveis em decorrência do potencial discriminatório e abusivo de seu tratamento, a depender do contexto de utilização das informações extraídas desses dados.

Diante da exposição dos princípios norteadores e hipóteses legais para o tratamento de dados pessoais – sensíveis e não sensíveis – podemos partir para a análise aprofundada da base legal que fundamentará a compreensão da ilicitude das práticas de entidades privadas vigilantes trazidas na seção I deste trabalho: o consentimento. Ademais, passaremos à compreensão de

[245] "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;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...)" – BRASIL. *Op. cit.*, 2018.
[246] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 139.

por que, **apesar de o consentimento não possuir primazia** sobre as demais bases legais, **possui primazia ímpar no presente trabalho**.

4.3 – O consentimento: motivos de sua aplicação, adjetivações da LGPD e diálogo com o GDPR

Antes de mais nada, vale memorar que o escopo de análise deste trabalho são as práticas de extração de dados pessoais realizadas por entidades privadas, a partir de três principais eixos de abordagem: i) Economia Comportamental, ii) Economia Psíquica dos Algoritmos, e iii) Neurociência. Sendo cada uma delas responsável por diversas repercussões psíquicas – abordadas na seção I – e jurídicas aos titulares de dados – que serão discorridas com profundidade no capítulo 5 desta seção.

A esta altura, cabe destacar que todas as obtenções e todos os tratamentos de dados mencionados na seção I são realizados por controladores configurados como pessoas jurídicas de direito privado, cujo objetivo primordial de pesquisa algorítmica e investimento em tecnologia é essencialmente o aumento de sua lucratividade. Tal finalidade, como visto anteriormente, quando atingida, é retroalimentada em um *feedback looping* positivo – em relação aos próprios controladores –, porém de externalidades muitas vezes negativas ao consumidor – enquanto titular de dados – que se vê, em contrapartida, diante de um *feedback looping* de injustiças (vide capítulo 2).

Torna-se, dessa feita, impossível justificar o tratamento de dados por entidades privadas vigilantes sob as hipóteses legais do artigo 7º, incisos III, IV, VI e VIII,[247] da LGPD. por exemplo; ou do seu artigo 11, inciso II, alíneas b, c, d e f[248] – respectivamente para dados não sensíveis e sensíveis. Além disso, não tratamos na seção I de hipóteses excepcionais em que as empresas de tecnologia têm de cumprir obrigação legal ou regulatória (art. 7º, I; art. 11, II, a) ou tratar dados para proteger a vida ou incolumidade física de titulares ou terceiros (art. 7º, VII; art. 11, II, e).

[247] Respectivamente as bases legais relativas ao tratamento pela Administração Pública para execução de políticas públicas; por órgãos de pesquisa para estudos; em hipóteses de exercício regular de direitos; e por profissionais de saúde para fins de tutela da saúde.
[248] Mesmas hipóteses elencadas na nota de rodapé anterior, porém para dados sensíveis.

Quanto às bases legais do legítimo interesse (art. 7º, IX) e de proteção ao crédito (art. 7º, X), veremos adiante no capítulo 5 que há algumas situações[249] em que estas podem ser utilizadas como requisitos de tratamento por companhias privadas no ambiente digitalizado, porém não nos moldes apresentados na seção I – isto é, de maneira abusiva e discriminatória.

Logo, resta evidente que, **para os tratamentos** de dados pessoais **realizados** pelas **empresas de tecnologia apresentados na seção I**, **a base legal adequada** para fundamentá-los é a do **consentimento** dos titulares. Tanto para dados sensíveis, quanto para dados não sensíveis, como ficará claro no capítulo 5 deste trabalho.

Nesse sentido, para que possamos compreender por que as técnicas manipulatórias apresentadas no capítulo 3 são juridicamente ilícitas de acordo com o ordenamento jurídico brasileiro, devemos destrinchar o entendimento desta base legal, preconizada no artigo 7º, inciso I, da Lei Geral de Proteção de Dados; bem como em seu artigo 11, inciso I. Em decorrência de o consentimento da LGPD ter como alicerce inspirador o preconizado pelo Regulamento Geral de Proteção de Dados europeu[250] (GPDR),[251] inevitável seria deixar de fazer certas comparações e alusões à legislação europeia no decorrer deste subcapítulo.

Primeiramente, vale rememorar que a LGPD define o consentimento em seu artigo 5º, inciso XII, como uma "**manifestação livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".[252] Além de, em hipóteses que configurem vulnerabilidade ou que indiquem maior grau de proteção ao titular – a exemplo do tratamento de dados sensíveis –, a lei ainda o designa como **específico e destacado**.[253]

Toda essa adjetivação em torno do consentimento, segundo Bruno Bioni, desencadeia uma estrutura dinâmica obrigacional em torno das relações jurídicas entre as partes interessadas em, de um lado, explorar dados pessoais por meio desta base legal e, de outro, "exercer um controle sobre tal manipulação".[254] Diante disso, o bem jurídico tutelado, ainda de acordo com

[249] **Será pormenorizado no capítulo 5 como pode se dar o uso dessas bases legais pelas empresas de tecnologia, a partir de exemplos práticos em que há uma relação prévia entre usuário e plataforma para fins de marketing direto – para a base do legítimo interesse – e através do que diz a Lei do Cadastro Positivo e a jurisprudência do Superior Tribunal de Justiça em relação ao *credit scoring* – para proteção ao crédito**.
[250] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 119.
[251] Em inglês, General Data Protection Regulation.
[252] BRASIL. *Op. cit.*, 2018. (grifos nossos)
[253] *Cf.*: Art. 11, I, LGPD.
[254] BIONI. *Op. cit.*, 2021, p. 181.

Bioni, seria justamente garantir que o elemento volitivo de manifestação de vontade seja "livre e consciente",[255] sob risco de ser declarada sua nulidade em caso de vício.[256]

O consentimento como um processo[257] de fomento à autodeterminação informacional do titular permite a parametrização de balizas necessárias para alcançar a **validade** desta base legal, balizas estas que na LGPD se configuram transvestidas de adjetivos: **livre, informado, inequívoco e específico**.[258] Passemos à elucidação de cada um deles.

4.3.1 – O consentimento livre

A principal característica do consentimento livre é real opção do titular de aceitar ou não o tratamento de seus dados pessoais,[259] sem coerção ou outros meios que possam viciar o processo de tomada de decisão. Deve-se, dessa feita, verificar qual o nível da assimetria informacional em jogo,[260] para que então se possa constatar o "poder de barganha"[261] do titular frente aos agentes de tratamento.

Esse poder visa a afastar a lógica binária das chamadas políticas tudo ou nada[262] – *take-it or leave-it* – imposta aos titulares, cuja utilização proporciona um tolhimento de sua liberdade de escolha na sociedade de informação, ainda mais considerando os aspectos manipulatórios constatados na seção I. Nessa senda, as opções disponíveis para a coleta do consentimento dos titulares, enquanto sujeitos em um capitalismo de vigilância datificado, deve se tornar **granular**, isto é, **não pode estar vinculado a nenhum tipo de *bundling* ou *tying*.**

---

[255] *Ibid*., p. 183.
[256] O artigo 8º, inciso §3º, da LGPD enuncia expressamente que: "É vedado o tratamento de dados pessoais mediante vício de consentimento. – BRASIL. *Op. cit*. 2018.
[257] *Cf*.: BIONI, Bruno Ricardo; LUCIANO, Maria. O consentimento como processo: em busca do cometimento válido. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, pp. 147-159.
[258] Em comparação, o GDPR, em seu artigo 4 (11), define o consentimento como: "(...) uma **manifestação 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" (grifos nossos) - UNIÃO EUROPEIA. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Art. 4 (11)**:** Definitions, 2016. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>, Acesso em: 07 dez. 2022.
[259] SANTOS, Isabela de Araújo. *A vulnerabilidade dos titulares de dados diante de grandes plataformas digitais e big techs*: um paralelo entre as violações ao GDPR e à LGPD no que tange à base legal do consentimento. Brasília: Revista dos Estudantes de Direito da Universidade de Brasília, 2022, p. 254.
[260] BIONI. *Op. cit*., 2021, p. 189.
[261] Bioni utiliza-se desses vocábulos para considerar as opções dos titulares em relação aos tipos de dados coletados pelos controladores e aos possíveis tratamentos realizados por estes e por operadores – *Idem*.
[262] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 121.

Esses termos foram introduzidos pelas Guidelines de nº 5 do European Data Protection Board (EDPB), da Diretiva 95/46 da União Europeia, e significam respectivamente, em uma tradução literal, **empacotamento e amarração**. Assim, pode-se inferir que o consentimento não deve ser associado a nenhum tipo de "empacotamento" de aceitação de termos ou condições de serviço, nem a nenhuma "amarração" a previsões contratuais ou a produtos e serviços que não sejam necessários para a plena eficácia do contrato.[263]

Diante disso, decorrem duas premissas importantes: i) a primeira é que a base legal do consentimento não pode de maneira alguma ser confundida com a de execução de contratos – a fim de que seja resguardado ao máximo o livre-arbítrio dos titulares no processo de tomada de decisão, de acordo com a devida informação das finalidades de tratamento[264] –; e ii) a segunda, que é necessária uma **vinculação objetiva** entre o **processamento** dos dados pessoais e as **finalidades** para as quais foi adquirido o consentimento.

Desse modo, quando uma plataforma digital ou *big tech* oferece um serviço que envolve múltiplos tratamentos de dados para mais de um fim, há a necessidade de que o titular e eventual fornecedor dos dados possa escolher quais dados ele permite serem processados, em vez de ter de consentir por todo um pacote de dados para diversos propósitos. O consentimento deve ser dado para cada um deles, devendo haver, portanto, granularidade.[265]

Logo, a granularização do consentimento abre espaço para a livre escolha do titular diante de um "fatiamento"[266] de funcionalidades ofertadas para o tratamento de seus dados pessoais, de acordo com as finalidades que os controladores desejam alcançar com este processamento.

Ademais, o adjetivo "livre" escolhido pela LGPD para caracterizar essa hipótese de tratamento ainda **abarca** as situações em que o titular decide revogar a autorização de tratamento de seus dados pessoais. Essa **revogação**, à semelhança do GDPR, pode ser feita a

---

[263] *Cf.*: UNIÃO EUROPEIA. *Guidelines 05/2020 on consent under Regulation 2016/679*, Adopted on 4 May 2020, p. 10. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt>, Acesso em: 7 dez. 2022.

[264] SANTOS, *Op. cit.*, Revista dos Estudantes de Direito da Universidade de Brasília, 2022, p. 254.

[265] "Um caso que exemplifica claramente uma situação não granular de consentimento é a situação em que uma loja pede o consentimento dos seus clientes cadastrados para fornecer dados a fim de enviar-lhes, por e-mail, as ofertas do mês e, concomitantemente, para divulgar esses mesmos dados com outras lojas do mesmo grupo empresarial para finalidades de *marketing*. Considerando que, nessa situação, não houve separação de autorizações para cada finalidade, não houve granularidade no requerimento do consentimento." – Ibid., p. 255.

[266] BIONI. *Op. cit.*, 2021, p. 189.

qualquer momento mediante manifestação expressa do titular, por **procedimento gratuito e facilitado**.[267] A legislação europeia ainda acrescenta que a revogação – *withdraw* – do consentimento deve ser realizada **sem nenhum detrimento**, isto é, tem de ser feita por meio e por ação de **igual facilidade e acessibilidade** quanto às que proporcionaram o seu fornecimento,[268] além de não ser eivada de coerção, intimidação ou ameaça.[269]

Todavia, para que os titulares possuam o mínimo de poder de barganha diante da assimetria de poder informacional existente entre eles e os controladores de dados que coletam seu consentimento, tornou-se necessário inserir um dever de informação por parte de quem deseja processar os dados a quem tem seus dados processados, para garantir ao máximo o elemento volitivo no processo de tomada de decisão.

Nesse sentido, perpassemos então pelas características do consentimento informado.

4.3.2 – O consentimento informado

Para que o consentimento do titular seja informado, as informações passadas dos agentes de tratamento a ele devem ser "necessárias e suficientes"[270] para que a tomada de decisão concernente à autorização da coleta de dados para determinadas finalidades seja feita de maneira livre e consciente. Para tanto, o titular tem de estar capacitado a controlar seus dados, devendo o fluxo de dados da cadeia de tratamento "tomar forma",[271] isto é, ser informado.

Tal decomposição do vocábulo informar em "colocar em forma" é empregada na seara do direito do consumidor,[272] podendo também ser utilizada no campo da proteção de dados pessoais, visto que o dever-direito de informação deve assegurar "os elementos necessários para o início de um processo de tomada de decisão no que tange ao fluxo"[273] informacional. Logo, partindo da concepção de que informar é dar forma ao ato de comunicação, este deve ser ostensivo e somatório.[274]

---

[267] E ainda ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação. *Cf.*: Art. 8º, §5º, da LGPD.
[268] *Cf.:* UNIÃO EUROPEIA. *Op. cit*., 2020, pp. 23-25.
[269] *Ibid.*, p. 11.
[270] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 122.
[271] BIONI. *Op. cit*., 2021, p. 184.
[272] *Cf.*: MARQUES, Claudia Lima; BENJAMIN, Antônio Herman; MIRAGEM, Bruno. Comentários ao Código de Defesa do Consumidor. 3ª ed. São Paulo: RT, 2010, p. 249.
[273] BIONI; LUCIANO. *Op. cit*., 2023, p. 151.
[274] Cf.: BIONI. *Op. cit*., 2021, pp. 184-185.

Isso porque não basta apenas um ato comunicacional vago e simplista para que o dever de informação seja cumprido como uma substancialização da autoproteção[275] do titular de dados, devem ser utilizados meios para **garantir uma informação que some e acresça o repertório informacional do titular** – para diminuir a assimetria entre ele e os agentes de tratamento.

Bruno Bioni pontua que é evidente que o titular jamais alcançará o **mesmo nível informativo dos controladores e operadores**, porém adiciona que é **desnecessário que saiba todas as minúcias da atividade da cadeia de tratamento;** mas sim que **compreenda "os riscos e as implicações que tal atividade trará sobre a sua esfera pessoal,** a fim de racionalizar sua decisão sobre o fluxo de seus dados"[276] (grifos nossos). Até porque, como visto na seção I deste trabalho, uma **sobrecarga de informações não significa necessariamente um melhor processo de tomada** de decisões no capitalismo de vigilância datificado – devendo ser diferenciado até que ponto a informação deixa de ser informativa e passa a ser deformadora, bem como em que medida a comunicação de transforma de comunicativa para meramente cumulativa.[277]

A adoção de *Privacy Enhancing Technologies* (PETs)[278] pode ser uma boa alternativa para controladores e operadores adimplirem com o dever de informação que têm para com os titulares de dados, porquanto essas tecnologias oferecem interfaces e mecanismos facilitadores de comunicação. As PETs, que se utilizam da inteligência artificial, podem, através de animações gráficas ou por meio de *plug-in* de leitura,[279] destacar e sumarizar pontos relevantes de termos de consentimento aos usuários de plataformas digitais e *big techs*, otimizando a **transparência** da informação que é transmitida dos controladores aos titulares de dados.

---

[275] Termo usado por: BARBOSA, Fernanda Nunes. Informação: direito e dever nas relações de consumo. São Paulo: Revista dos Tribunais, 2008, p. 35.
[276] BIONI. *Op. cit*., 2021, p. 185.
[277] Tal entendimento, como elucidado na seção I, está contido na obra No Exame, de Byung-Chul Han. *Cf.*: HAN. *Op. cit*., 2018, p. 106.
[278] As PETs podem ser definidas como "soluções de software e hardware (tecnologias), bem como métodos ou conhecimentos para proteger contra riscos de privacidade." (Tradução livre) – *Cf.*: E-SPIN. Types of Privacy Enhancing Technologies and their examples. *In: Global Themes and Features Topics, Industries, Information Technology*, publicado em 18. nov. 2021. Disponível em: <https://www.e-spincorp.com/types-of-privacy-enhancing-technologies-and-their-examples/>. Acesso em 15. dez. 2022.
[279] Exemplos trazidos por Bruno Bioni para sistematizar o uso de PETs para otimizar a experiência do titular de dados no processo de tomada de decisão no que tange o aceite de políticas de privacidade. Vide: BIONI. *Op. cit*. 2021, p. 187.

Quanto à transparência da informação, a LGPD é clara ao estabelecer uma lógica qualitativa e quantitativa[280] que a caracterizaria. Quanto ao aspecto qualitativo, o *caput* do seu artigo 9º estabelece que "[o] titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas **de forma clara, adequada e ostensiva** acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso" (grifos nossos).

No que concerne aos aspectos quantitativos, a lei elencou, nos incisos do mesmo artigo, um **rol exemplificativo da quantidade mínima de informações** que os agentes de tratamento devem passar ao titular para a garantia da transparência, do acesso facilitado e, por conseguinte, do livre acesso aos seus dados pessoais. Dessa feita, o titular tem o direito de ser informado quanto a: i) finalidade determinada do tratamento; ii) forma e duração do tratamento – isto é, ciclo de vida dos dados –, resguardados os segredos comercial e industrial; iii) quem é (são) o(s) controlador(es) dos dados; iv) quais os contatos do(s) controlador(es); v) informações sobre usos secundários dos seus dados feitas pelo(s) controlador(es) e quais as finalidades ulteriores; vi) quais são as responsabilidade de cada agente (controladores, operadores e terceiros) que realizarão o tratamento; e vii) quais são os seus direitos como titular, devendo haver referência explícita ao artigo 18[281] da LGPD.

---

[280] Cf.: *Ibid*., p. 188,

[281] O artigo 18 da LGPD está contido no seu Capítulo III, que contém a enumeração e explicação dos direitos dos titulares de dados pessoais: "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
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, nos termos do § 5º do art. 8º desta Lei.
§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Desse modo, percebe-se que o principal escopo da inserção do artigo 9º na estrutura normativa da LGPD foi a de **reduzir a assimetria informacional**, ao almejar a **eliminação de obscuridades e opacidades**[282] por parte dos agentes de tratamento que pudessem ocasionar em um travamento do fluxo de dados pessoais em relação à **comunicação clara, transparente e necessária** com os titulares.

Toda essa prestação de informações, da maneira elucidada, tem direto impacto no modo como são apresentadas as finalidades de tratamento dos dados pessoais pelos controladores aos titulares. Afinal, para que não haja obscuridade e opacidade informacional quanto às razões que levaram os controladores a perseguirem as finalidades propostas, estes devem transmitir as informações cabíveis aos titulares para que estas que possam auxiliá-los em sua tomada de decisão, de modo que façam isso de maneira **inequívoca**.

Analisemos, portanto, como deve ser configurado o consentimento inequívoco.

4.3.3 – O consentimento inequívoco

O adjetivo inequívoco possui uma conotação de "**não manipulação**"[283] do titular e ainda de "**não ambiguidade**"[284] da informação que lhes é comunicada pelos agentes de tratamento. Isso significa que toda declaração de vontade deve ser vinculada a um direcionamento que, além de livre e informado, n**ão pode ser alicerçado em finalidades genéricas e vazias**.[285] Em adição, as Guidelines de nº 5 do EDPB enunciam que o consentimento requer um **ato positivo claro**[286] para se demonstrar como inequívoco, de modo

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor." – BRASIL. *Op. cit.*, 2018.

[282] BIONI; LUCIANO. *Op. cit.*, 2023, p. 152.

[283] BIONI. *Op. cit*., 2021, p. 190.

[284] *Cf.*: SANTOS, *Op. cit*., Revista dos Estudantes de Direito da Universidade de Brasília, 2022, p. 256.

[285] Cf.: BIONI. *Op. cit.*, 2021, p. 190,

[286] Para isso, não necessariamente o titular deve assinar ou escrever que consente com o tratamento para as finalidades determinadas, podendo ser feito o aceite por preenchimento de formulário eletrônico, assinatura eletrônica ou por interfaces de *finger swipe*, por exemplo. Vide: UNIÃO EUROPEIA. *Op. cit.*, 2020, pp. 18-19.

que "o silêncio ou a mera falta de manifestação por parte do titular não podem ser consideradas formas de obtenção de seu consentimento."[287]

Um claro exemplo em que se configura ambiguidade de tomada de decisão é o caso de pré-seleção de opções de caixas de configurações de privacidade[288] e de *cookies*, em que pode se afirmar que o titular restaria silente quanto à vontade de ter seus dados processados para as finalidades propostas. Isso porque Goldbeck e Mauriello constataram que a maioria das pessoas que utilizam mídias sociais – especificamente o Facebook – tendem a ignorar os termos de uso e as políticas de privacidade contidas à sua disposição.[289] Dos resultados da pesquisa, puderam averiguar que apenas 2.21% dos usuários entrevistados de fato leem os contratos de adesão[290] [291] antes de aceitá-los, o que repercute diretamente em um déficit informacional dos titulares.

Tal imposição de assimetria da informação, como já discorrido, não é meramente ocasional, visto que as plataformas digitais e *big techs* poderiam se utilizar de PETs com interfaces mais adequadas e amigáveis para proporcionar uma melhor comunicação com seus usuários e motivá-los a se engajar mais no conhecimento de seus direitos como consumidor e titular de dados pessoais – o que demonstra um cenário claramente abusivo e manipulatório por parte dessas empresas (vide seção I).

Logo, nos termos de Bruno Bioni, o que deve ser avaliado para que o consentimento do titular seja de fato inequívoco, isto é, para que tenha um **controle visceral**[292] **sobre seus dados pessoais**, é "o grau e a qualidade da interação do usuário"[293] com o *design* do ambiente de tomada de decisão, o que torna essa adjetivação intrinsecamente ligada ao **princípio da boa-fé** da LGPD – depositando, inclusive, no controlador o ônus de provar que o consentimento foi fornecido em conformidade com os dispositivos legais.[294]

---

[287] SANTOS, *Op. cit*., Revista dos Estudantes de Direito da Universidade de Brasília, 2022, p. 256.
[288] Exemplo trazido por: BIONI. *Op. cit*., 2021, p. 191.
[289] GOLDBECK, Jennifer; MAURIELLO, Matthew. *User perception of Facebook app data access: a comparison of methods and privacy concerns*. Future Internet, v. 8, n. 2, 106, p. 9.
[290] De uma amostra de 120 entrevistados, foi possível constatar apenas esse percentual. Cf.: GOLDBECK; MAURIELLO. *Op. cit*., 2016, p. 4.
[291] Segundo o Código de Defesa do Consumidor, no caput de seu artigo 54, contratos de adesão são os negócios jurídicos "cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo." – BRASIL. *Lei nº 8.078, de 11 de setembro de 1990.* Dispõe sobre a proteção do consumidor e dá outras providências, Brasília, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 17 dez. 2022.
[292] Termo utilizado por: CALO, Ryan. *Against notice skepticism in privacy (and elsewhere).* Notre Dame Law Review, v. 87, n. 3, 2011, pp. 1027-1072.
[293] BIONI. *Op. cit*., 2021, p. 192.
[294] Cf.: Art.8º, §2º, da LGPD.

Entretanto, vale lembrar que o legislador ainda considerou a existência de situações em que, mesmo que o titular possa fornecer um consentimento livre, informado e inequívoco, cabe à LGPD proporcionar uma "camada adicional de proteção" aos seus direitos e salvaguardas, visto configurarem hipóteses de elevados riscos. Para isso, foi estabelecido mais um adjetivo para caracterizar o consentimento: específico, cuja examinação será realizada adiante.

4.3.4 – O consentimento específico

A fim de que deva ser configurado como específico, o consentimento tem de estar condicionado às hipóteses taxativas apresentadas na Lei Geral de Proteção de Dados, quais sejam: i) o tratamento de **dados sensíveis** do titular;[295] ii) o **envolvimento de terceiros** na cadeia de tratamento que não possuem relação direta com o titular;[296] iii) as situações que envolvam o tratamento de **dados de crianças e adolescentes**;[297] e iv) a **transferência internacional** de dados para países que não possuam o mesmo nível de proteção de dados pessoais que o Brasil.[298]

O maior nível de proteção a essas situações pontuais garante uma maior assertividade[299] do titular diante de maiores possibilidades de riscos a seus direitos e garantias legais e constitucionais. Dessa feita, os agentes de tratamento possuem o dever de assegurar maior nível de participação do titular no seu processo de tomada de decisão, a partir de mecanismos de **especificidade e destaque** das cláusulas contratuais de **consentimento**.

A especificidade pode ser entendida como uma conjunção entre a transparência de determinação dos propósitos concretos de tratamento e as obrigações de granularidade para obtenção do consentimento por parte dos controladores. O destaque, por sua vez, há de ser compreendido como uma necessidade de se priorizar o pleno acesso do titular às informações dos fatos relevantes do tratamento,[300] principalmente no que tange aos riscos do processamento.

Quanto ao tratamento de dados sensíveis, vale pontuar que a aplicação do artigo 11 da LGPD pode ser feita para dados pessoais que não sejam, *prima facie*, sensíveis. Isso porque dados não sensíveis podem vir a se tornar sensíveis dependendo do contexto de tratamento, a

[295] Hipótese prevista pelo art. 11, I, da LGPD.
[296] Vide*:* Art. 7º, §5º, da LGPD.
[297] Vide: Art. 14, §1º, da LGPD.
[298] Vide: Art. 33, VIII, da LGPD.
[299] BIONI. *Op. cit*., 2021, p 193.
[300] As definições podem ser conferidas em: VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 141.

partir do momento que puderem ser inferidas informações desse tipo a respeito dos titulares. Nas palavras de Ana Frazão,

> [A] linha distintiva entre dados pessoais e dados pessoais sensíveis pode não ser tão nítida, até porque a perspectiva de **análise deve ser dinâmica e não estática**. Dessa maneira, há boas razões para sustentar que são sensíveis todos os dados que permitem que se chegue, como resultado final, a informações sensíveis a respeito das pessoas.[301] (grifos nossos)

Portanto, **o consentimento específico pode vir a ser aplicado também a dados que podem ainda vir a ser caracterizados como sensíveis**, a depender do tipo de tratamento que será realizado e de acordo com as finalidades pretendidas.

Diante do elucidado, foi possível averiguar as características que regem os pressupostos de validade da base legal do consentimento. As adjetivações da LGPD, comparativamente às diretrizes estabelecidas pelo GDPR, viabilizam uma melhor compreensão desta hipótese autorizativa de tratamento. Ao conjugarmos essas noções aos princípios basilares que orientam o tratamento de dados pessoais, será possível analisar com maior acurácia a ilicitude das práticas apresentadas na seção I deste trabalho.

Antes, porém, torna-se interessante frisar que a concepção de consentimento do titular não é abordada apenas pela LGPD no ordenamento jurídico brasileiro, havendo menções em outros dispositivos normativos, tais como o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet (MCI). Importante pontuar que o CDC e o MCI trazem ainda outros aspectos relevantes relativos a direitos e garantias a titulares de dados que merecem especial destaque neste trabalho, cujo foco será dado no subcapítulo seguinte.

4.4 – O Código de Defesa do Consumidor e o Marco Civil da Internet: vulnerabilidade do consumidor-cidadão, diálogo de fontes e dados cadastrais

A Lei nº 8.078/1990, doravante Código de Defesa do Consumidor (CDC), assim como a LGPD, considera a vulnerabilidade de titulares de dados, enquanto consumidores,[302] diante

[301] FRAZÃO, Ana. *Nova LGPD*: o tratamento dos dados pessoais sensíveis. Jota, publicado em 26 set. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em 16 dez. 2022.

[302] Consumidor, para o CDC, é "toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final" e ainda "a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo". Vide: Art. 2º, *caput* e § único, do CDC. – BRASIL. *Op. cit.*, 1990.

da assimetria informacional existente entre eles e seus fornecedores de produtos e serviços,[303] que podem ser configurados como controladores de dados pessoais – a depender do contexto de tratamento.

Segundo Claudia Lima Marques e Bruno Miragem, em relações consumeristas, o controlador pode ser o próprio fornecedor de produtos e serviços quando este coletou os dados de seus consumidores para fomentar suas decisões negociais ou quando for o próprio "gestor do banco de dados ao decidir formatar determinadas informações que diretamente coletou ou recebeu por intermédio de compartilhamento."[304] Para os autores, o que define a posição de controladoria na relação de consumo é o poder de decisão sobre os dados, bem como as repercussões que essa atuação terá sobre os interesses dos titulares como consumidores.[305]

Dessa feita, pode-se notar que os autores introduzem um diálogo de fontes[306] entre LGPD e CDC para conciliar ambos diplomas normativos harmonicamente, considerando o ordenamento jurídico brasileiro plúrimo e a necessidade de se coordenar as leis para que se atinja um sistema eficiente, coerente e justo.[307] Essa convergência normativa possui origem legal e, de acordo com Laura Schertel e Danilo Doneda, tem como finalidade a arquitetura de um conjunto normativo de proteção de dados aos consumidores:

> A Lei 13.709/2018 – **Lei Geral de Proteção de Dados Pessoais (LGPD)** [...] inaugura no Brasil um regime geral de proteção de dados pessoais. A referida Lei vem complementar o marco regulatório brasileiro da Sociedade da Informação ao compor, **juntamente com** a Lei de Acesso à Informação, **o Marco Civil da Internet e o Código de Defesa do Consumidor, o conjunto normativo que moderniza o tratamento da informação no Brasil.** Seu objetivo é proporcionar garantias aos direitos do cidadão, ao mesmo tempo que fornece as bases para o desenvolvimento da

[303] "Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
§ 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
§ 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista." – *Idem*.
[304] MARQUES, Claudia Lima; MIRAGEM, Bruno. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor e os novos direitos do consumidor-titular dos dados. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 806.
[305] *Ibid*., pp. 806-807.
[306] Inspirando-se em Erik Jayme, Claudia Lima Marques e Bruno Miragem definem-no como: "'Diálogo das fontes' é uma expressão visionária, que destaca a força da Constituição (e dos Direitos Fundamentais), assim as fontes plurais não mais se excluem – ao contrário, mantêm as suas diferenças e narram simultaneamente suas várias lógicas [...], cabendo ao aplicador da lei coordená-las [...], impondo soluções harmonizadas e funcionais no sistema, assegurando efeitos úteis a estas fontes, ordenadas segundo a compreensão imposta pelo valor constitucional." – *Ibid*., p. 797.
[307] *Cf.*: JAYME, Erik. Identité culturelle et intégration: le droit internationale privé postmoderne. In: JAYME, Erik. *Recueil des Cours de l'Académie de Droit International de La Haye*. Doordrecht: Kluwer, 1995, pp. 60-61.

> economia da informação, baseada nos vetores da confiança, segurança e valor.[308] (grifos nossos)

Percebe-se, assim, que além do CDC, a coadunação de fontes com a LGPD ocorre também com a Lei nº 12.965/2014, o denominado Marco Civil da Internet (MCI). Ambos os diplomas normativos conferem, assim como a Lei Geral de Proteção de Dados, salvaguardas aos titulares, capazes de incrementar seus direitos diante de sua situação de vulnerabilidade[309] no capitalismo de vigilância datificado, o que terá relevância direta na análise das práticas subreptícias por parte das empresas de tecnologias no capítulo 5 deste trabalho. Portanto, passemos a analisar como o CDC e o MCI conferem mecanismos de proteção aos titulares de dados.

Inicialmente, insta salientar que ambas legislações fazem **menção ao consentimento** do titular como pré-requisito de garantia de uma **mínima simetria informacional** entre o consumidor-cidadão e o fornecedor de produtos e serviços. **No CDC**, podemos extrair essa noção a partir da leitura de seu **artigo 6º, incisos II e III**, que preconizam a **liberdade de escolha e igualdade** nas contratações, bem como a comunicação entre fornecedores para com seus consumidores a partir de **informações claras e adequadas** – a partir da especificação correta sobre quantidade, característica, composição, riscos, dentre outros fatores que possam afetar diretamente os consumidores.[310] Além de notarmos uma clara convergência com os princípios da LGPD da **adequação, transparência, qualidade dos dados e do livre acesso**, há uma aproximação visível entre a noção de consentimento informado da referida lei com a do CDC.

Com relação ao **MCI**, em seu **artigo 7º, inciso IX**, esse diploma normativo faz **referência direta** à necessidade de se **coletar o consentimento expresso** do cidadão como um direito ao **livre acesso à internet**, direito este que deve estar **destacado das demais cláusulas contratuais**.[311] A semelhança com o consentimento específico e destacado pormenorizado pela LGPD não é mera coincidência, sendo que a utilização do termo "expresso" pela norma de proteção de dados – à imagem do MCI e da Diretiva 95/46 da União Europeia – foi defendida por alguns autores da doutrina brasileira,[312] por ser mais adequado do que o termo "específico"

---

[308] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, pp. 469-493, nov.-dez., 2018, pp. 469-470.
[309] Vide: Art. 4º, I, do CDC; e Arts. 2º, II; 4º, I e II, do MCI.
[310] Vide: Art. 6º, II e III, CDC. – BRASIL. *Op. cit.*, 1990.
[311] Vide: Art. 7º, IX, MCI. – BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 17 dez. 2022.
[312] Para mais informações, *cf.*: BIONI. Op. cit., 2021, p. 194.

para designar situações em que o nível de assertividade do titular deve ser tutelado com mais afinco.

Além das minúcias relativas a essa base legal, o MCI também dialoga com a LGPD no sentido de almejar a prestação de informações claras e completas nos contratos de prestação de serviços entre fornecedores e consumidores sobre práticas de gerenciamento de rede,[313] assim como sobre a coleta, o uso e tratamento de dados pessoais, de acordo com **finalidades determinadas**.[314] Vê-se, nesse sentido, novamente uma coadunação com a principiologia contida na Lei Geral de Proteção de Dados, neste ponto com destaque para os princípios da **finalidade** e da **necessidade**.

Ademais, cabe pontuar que o Código de Defesa do Consumidor estimula a relação de equilíbrio entre fornecedores e consumidores a partir da **prática da boa-fé objetiva contratual**,[315] **vedando** qualquer tipo de **publicidade enganosa ou abusiva**, sendo consideradas **nulas cláusulas** contratuais que estabeleçam **obrigações incompatíveis** com a boa-fé ou com a equidade – de acordo com o artigo 51, inciso IV, do CDC.

Vale memorar que a **publicidade enganosa** constitui a informação passada ao consumidor **inteira ou parcialmente falsa** que, mesmo por caráter omisso, possa **induzi-lo a erro** a respeito da natureza e demais características do produto ou serviço – art. 37, §1º e 3º, do CDC. Em complementação, a **publicidade abusiva** é caracterizada pela informação publicitária **discriminatória** que incite violência ou explore medo, aproveitando-se de deficiência de julgamento e de experiência de criança ou desrespeitando valores ambientais, bem como aquela que induz o consumidor a tomar **atitude comportamental nociva** a sua própria saúde ou segurança – artigo 37, §2º, do CDC.

Nesse sentido, o alicerce principiológico da LGPD – localizado no *caput* do seu artigo 6º – encontra também relevância central no CDC, indicando mais uma vez uma harmonização dialógica normativa entre as mencionadas legislações.

Ainda, resta evidenciar que o Marco Civil da Internet e o Código de Defesa do Consumidor preveem a possibilidade de acesso a banco de dados cadastrais por parte dos titulares a fim de obterem informações concernentes a seu respeito, bem como sobre as fontes

[313] Vide: Art. 7º, VI, MCI.
[314] Vide: Art. 7º, VIII, MCI.
[315] Vide: Art. 4º, III, do CDC.

dos dados extraídos dessas informações – arts. 43, *caput* e §1º, do CDC; e 10, §3º, do MCI. Essas informações podem estar contidas em dados pessoais de cadastros, fichas e registros que devem prezar pela objetividade, clareza, veracidade e linguagem de fácil compreensão; não podendo conter informações negativas referentes a período superior a cinco anos, nem dados desatualizados de reclamações fundamentadas contra fornecedores de produtos e serviços – arts. 43, §1º; e 44, *caput*, do CDC.

Por fim, um tema que merece especial atenção neste ponto, justamente por envolver o direito de acesso a base de dados por parte dos consumidores, é o do ***credit scoring***, que pode ser definido como um "sistema de pontuação utilizado pelas instituições que operam com relações comerciais ou creditícias, que tem como finalidade auxiliar na tomada de decisões relativas à concessão de crédito a determinado consumidor".[316] Essa prática, que trata dados pessoais referentes a idade, estado civil, sexo, profissão, renda e histórico de adimplemento de consumidores,[317] foi **considerada lícita pelo Superior Tribunal de Justiça (STJ)** no julgamento do Recurso Especial nº 1.419.697, com fundamento nos artigos 5º, inciso IV, e 7º, inciso I, da Lei nº 12.414/2011 – denominada **Lei do Cadastro Positivo**.

Na referida decisão, o entendimento firmado pelos Ministros foi de que, apesar de ser **desnecessária a coleta do consentimento** do titular para as avaliações de risco de crédito segundo a Lei do Cadastro Positivo, há de ser respeitada a **transparência** das relações negociais entre fornecedores e consumidores-titulares. Disso decorre o dever de **prestar os esclarecimentos solicitados pelo consumidor**, tanto acerca dos dados relativos a ele, quanto a respeito da fonte das informações.[318]

Cabe ressaltar que **a Lei nº 12.414/2011 proíbe** o registro de **informações excessivas**, isto é, aquelas que não sejam estritamente necessárias para a avaliação do risco creditício por parte das instituições deste setor econômico, assim como de dados sensíveis. O princípio da **necessidade** é empregado pelo legislador como uma maneira de se **evitar atos discriminatórios** por meio de abuso de direito a partir da prática do *credit scoring*, o que

[316] VIOLA; TEFFÉ. *Op. cit.*, 2023, p. 136.
[317] *Idem.*
[318] BRASIL. Superior Tribunal de Justiça, *REsp 1.419.697/RS*, Rel. Min. Paulo de Tarso Sanseverino, Brasília. Data de Julgamento: 12/11/2014. Data de Publicação DJe: 17/11/2014. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=39037908&num_registro=201303862850&data=20141117&tipo=51&formato=PDF>. Acesso em: 17 dez. 2022.

poderia ocasionar riscos altíssimos aos titulares de dados cuja única opção de não participação nesse tipo de tratamento constitui em um mecanismo de *opt-out*.[319]

Assim, diante do arcabouço jurídico de proteção aos titulares de dados apresentado neste capítulo, podemos adentrar, com maior grau de detalhamento, nas especificidades das práticas sub-reptícias das entidades privadas vigilantes, abordadas nos capítulos 2 e 3 deste trabalho. Veremos adiante por que, de acordo com as legislações apresentadas e tendo como ponto de partida o direito fundamental à proteção de dados pessoais, as empresas de tecnologia violam massivamente o consentimento e diversas salvaguardas dos titulares, enquanto consumidores e cidadãos inseridos em uma ordem constitucional democrática.

[319] Ou seja, de retirada voluntária de seus dados do sistema das instituições, e não de um consentimento autorizativo pré-tratamento (*opt-in*).

CAPÍTULO 5 – Análise jurídica das práticas manipulatórias

Iniciaremos o exame, sob a óptica jurídica, das técnicas manipulatórias apresentadas na seção I a partir dos exemplos de práticas de persuasão utilizadas por plataformas digitais, *big techs* e demais companhias vigilantes do ambiente digitalizado contra titulares de dados trazidos ao longo deste trabalho. Primeiramente, analisaremos as técnicas do campo da Economia Comportamental, em seguida da Economia Psíquica dos Algoritmos e da Neurociência (vide capítulo 3), empregadas – em sua maior parte – por empresas de tecnologia; para, então, finalizarmos este capítulo no estudo de situações que envolvem entidades privadas de outros setores da economia (relativas a exemplos trazidos no subcapítulo 2.2).

Já foi estabelecido no subcapítulo 4.3 que, para as situações abordadas neste trabalho, a base legal que deve ser utilizada como hipótese de licitude do tratamento de dados pessoais pelas empresas – tanto as do setor tecnológico, quanto as dos demais ramos econômicos – é a do consentimento. Partiremos dessa premissa para realizar a análise jurídica, baseada nas legislações apresentadas no capítulo 4 deste trabalho – realizando as ressalvas necessárias em casos de concorrência com outras bases legais estipuladas pela LGPD.

5.1 – Configuração da ilicitude de *dark patterns* e suas ameaças aos direitos dos titulares de dados pessoais

Como visto no subcapítulo 3.1, as *dark patterns* são os padrões obscuros utilizados pelo processamento algorítmico para **dificultar o processo de tomada de decisão livre e consciente** dos indivíduos. Por isso, têm intrínseca relação com o *(hiper)nudge*, a partir do momento em que pré-selecionam a escolha dos titulares de dados, no que se refere à coleta do seu consentimento.

Ao **destacarem ou esconderem botões de opção de compra e preço de produtos ou serviços**, por exemplo, as *dark patterns* já **violam diretamente os artigos 5º, inciso XII, e 8º, §3º, da LGPD**, por não fornecerem ao titular uma manifestação de vontade livre de vícios, inequívoca – por constituírem *per se* uma técnica manipulatória – e informada – afinal, foi suprimida informação relevante do titular. Ademais, na seara consumerista, pode-se afirmar uma clara **violação ao artigo 6º, inciso III, do CDC**, por impedirem o fornecimento da comunicação adequada entre fornecedor e consumidor no que se refere ao preço de produtos e serviços.

No que tange às tipologias das *dark patterns*, podemos constatar violações específicas a cada uma delas. As ***dark patterns* de obstrução**, por serem caracterizadas por um *confirmshaming* explícito e por uma ameaça de **prejuízo** em caso de revogação de consentimento do titular, **vão de encontro com o artigo 8º, §5º, da LGPD; além de constituírem prática vedada pelas Guidelines de nº 5 do EDPB**.[320] Isso porque, como já visto (vide item 4.3.1), a revogação do consentimento deve ser concedida ao titular por procedimento gratuito e facilitado, sem nenhum detrimento, assim como por ação de igual facilidade e acessibilidade quanto às que proporcionaram o seu aceite – não podendo ser caracterizada por coerção, intimidação ou qualquer tipo de ameaça.

As ***dark patterns* incômodas**, à semelhança das anteriores, também **violam a garantia de revogação facilitada do consentimento**, visto que a aceitação de notificações e interfaces torna-se mais fácil ao titular em decorrência da insistência dos aplicativos e sites. A desproporção entre a viabilidade de fornecimento e revogação, desse modo, constitui violação do **artigo 8º, §5º, da LGPD**. Além disso, pode-se afirmar que essa tipologia não observa o **consentimento inequívoco (art. 5º, XII, LGPD)**, visto que manipula o titular pelo chamado "incômodo" – *nagging* –, utilizando-se de interfaces cujos *designs* são intencionalmente inóspitos ao titular para sua tomada de decisão.

Por sua vez, as ***dark pattern*s de isca e troca** têm repercussão direta nas garantias do titular de dados enquanto consumidor. Por surpreender o consumidor com preços diferentes dos ofertados ou barreiras de anúncios indesejados, esse tipo de *dark patterns* viola diretamente o **artigo 6º, incisos II e III, do CDC**, por não conferir liberdade de escolha e igualdade nas contratações, e muito menos informações adequadas e corretas em relação ao preço dos produtos e serviços ofertados. Ademais, pode-se constatar **a prática de publicidade enganosa (art. 37, §1º, CDC),** por justamente induzir o consumidor-titular a crer na informação publicitária errada relativa ao produto ou serviço ofertado; além de que o consentimento que porventura for coletado do titular estará novamente eivado de vício manipulatório, afrontando o **artigo 8º, §3º, da LGPD –** caracterizando vício de consentimento.

Por fim, as ***dark patterns* de evasão,** por constituírem fundamentalmente uma técnica para desviar a atenção e esconder informação relevante do titular, violam o **dever de prestação de informações necessárias e suficientes** que deve ser conferido a quem fornece seus dados

[320] UNIÃO EUROPEIA. *Op. cit*., 2020, pp. 23-25.

pessoais – o **consentimento informado**. Esses padrões obscuros tolhem o engajamento informacional do titular, tanto pela omissão de informação (**art. 9º, da LGPD**), quanto pela sobrecarga informacional, indo de encontro com o **artigo 6º, inciso IV, da LGPD** – ou seja, com o princípio da **transparência**.

Logo, nota-se que, apesar de aparentarem-se inofensivas, em um primeiro momento, as *dark patterns* podem ter repercussões jurídicas diversas e significativas, tanto no campo da proteção de dados pessoais, quanto no direito do consumidor. Isso porque seu viés manipulatório sofisticado, ao ser utilizado por empresas de diversos setores da economia digital, permite-lhes **transvestir a persuasão em carga participativa do consumidor-titular,** conferindo ao indivíduo a falsa sensação de liberdade e poder sobre suas escolhas diante de **opções pré-estabelecidas**.

Tal tolhimento da manifestação volitiva do titular, como já visto, não é lícito, de acordo com o ordenamento jurídico brasileiro, que preza pela livre, inequívoca e informada escolha por parte dos titulares de dados pessoais em relação ao tratamento das informações que lhe dizem respeito. Eis, portanto, um apanhado do que foi constatado até aqui sobre as violações referentes às *dark patterns*, para que possamos continuar a seguir com as práticas abordadas no subcapítulo 3.2:

Tabela 2 – Violações Jurídicas – *Dark Patterns*

DARK PATTERNS	
LGPD	**CDC**
Art. 5º, inciso XII (consentimento livre, inequívoco e informado)	Art. 6º, incisos II e III (liberdade de escolha e igualdade nas contratações; informações adequadas e corretas em relação ao preço dos produtos e serviços ofertados)
Art. 8º, §3º (vício de consentimento)	Art. 37, §1º (publicidade enganosa)
Art. 8º, §5º (revogação facilitada do consentimento)	**Guidelines nº 5 EDPB**

Art. 9º, *caput* e incisos (dever de informação)	Revogação do consentimento (por procedimento gratuito e facilitado)
Art. 6º, VI (princípio da transparência)	Revogação sem detrimento (igual facilidade e acessibilidade)

5.2 – Modelo do gancho e matematização das expressões faciais como violações ao consentimento dos titulares

Neste subcapítulo, iniciaremos a análise jurídica a partir das práticas manipulatórias da matriz captológica da Economia Psíquica dos Algoritmos para, em seguida, partirmos para a examinação da matriz preditiva comportamental. Importa rememorar, neste ponto, que Frank Pasquale afirmou, em *The Black Box Society*, que os controladores de dados pessoais, no capitalismo de vigilância datificado, priorizam a maximização de seus lucros em detrimento do tratamento adequado dos dados dos titulares,[321] violando diversas de suas garantias constitucionais e infraconstitucionais, como será demonstrado adiante.

5.2.1 – Práticas sub-reptícias da captologia comportamental

A mobilização e captura da atenção de usuários e consumidores constitui o principal mecanismo de atuação de plataformas e *big techs* que investem na economia da atenção (vide item 3.2.1). A influência no comportamento humano, de maneira a obter padrões desejados, a partir de uma arquitetura de ferramentas analíticas e práticas pode vir a constituir violações a direitos e garantias de titulares de dados pessoais.

Isso porque, se não adotadas salvaguardas adequadas de proteção aos usuários e consumidores, podem ser constatadas práticas abusivas por partes das empresas de tecnologia que se utilizam do denominado "**modelo do gancho**" de captura da atenção (vide item 3.2.1). Esse modelo, como já discorrido, é dividido em quatro etapas: gatilhos, ação, recompensas variáveis e investimento.

[321] PASQUALE. *Op. cit.*, 2015.

Em relação à primeira etapa, os **gatilhos** – que se subdividem em externos e internos – trazem implicações jurídicas que merecem especial atenção. Os **gatilhos externos**, por serem eminentemente constituídos pelo **envio massivo de notificações** aos usuários de plataformas digitais e *big techs*, representam uma ameaça ao **livre, inequívoco e específico consentimento** do titular (**art. 5º, XII, da LGPD**), caso a notificação não tenha sido **expressamente** autorizada em **cláusula destacada** das demais nos termos de uso e na política de privacidade do aplicativo ou *website* (**art. 7º, IX, do MCI**).

Além disso, cabe pontuar que esses contratos de adesão, caso sejam simplistas ou sobrecarreguem o titular com informações excessivas, a fim de confundi-lo ou manipulá-lo a aceitar seus termos e cláusulas, em uma política de "tudo ou nada" que não especifique as finalidades da coleta e tratamento dos dados pessoais, violam diretamente os **artigos 6º, I; e 9º, *caput* e incisos, da LGPD; bem como o artigo 6º, II e III, do CDC.** Isso porque é dever do controlador-fornecedor, além de prestar informações claras a respeito das finalidades do tratamento ao titular – de maneira adequada e ostensiva –, garantir o direito do titular-consumidor à liberdade de escolha e igualdade nas contratações a partir da transparência em relação às especificidades do produto ou serviço.

Os gatilhos externos podem ainda ter implicações nos tipos de notificação que os usuários de plataformas e *big tech*s gostariam de receber, sendo que os controladores que não observarem, em seus termos de uso e políticas de privacidade, a **granularidade do consentimento,** estarão indo de encontro com as **Guidelines de nº 5 do EDPB**. Como já visto, essas diretrizes da União Europeia estabelecem que o consentimento do titular de dados não pode estar vinculado a nenhum tipo de "**empacotamento" ou "amarração"** a previsões contratuais desnecessárias para as finalidades almejadas (**princípio da finalidade e da necessidade – art. 6º, I e III, da LGPD**).

Ainda em relação aos gatilhos externos, cabe frisar que se a revogação do consentimento para que o titular pare de receber as notificações não seja igualmente facilitada, acessível e gratuita quanto no momento de sua coleta, as plataformas digitais e *big techs* não observariam o **artigo 8º, §5º, da LGPD.** Neste ponto, vale remorar que já constatamos que o uso de *dark patterns* de *nagging* constituem uma violação do mesmo artigo, devendo ser vedadas para fins de constituir a primeira etapa do modelo do gancho.

No que concerne aos **gatilhos internos**, que, constituem a modelagem da atenção a partir da manipulação das emoções – geralmente negativas – dos usuários e consumidores, insta salientar que as principais violações legais constatadas são as dos **artigos 8º, §3º, da LGPD; e 4º, III, do CDC**. Isso porque, ao se valerem da persuasão de emoções dos titulares – a partir da coleta de seus dados geralmente através de *likes*, publicações e interesses – as plataformas digitais e *big techs* **enviesam o "poder de barganha"** do indivíduo (vide item 4.3.1), por viciarem eventuais fornecimentos de consentimento, além de priorizarem o **desequilíbrio informacional** entre fornecedor de serviços e consumidor – prática que coloca em xeque a harmonização entre ambos pautada pela **boa-fé,** preconizada pelo CDC.

A segunda etapa do modelo do gancho, por sua vez, caracterizada pela **ação** – ou seja, a observação e estímulo do comportamento "enganchado" dos usuários mediante os gatilhos –, bem como a terceira etapa de **recompensas variáveis** – que criam um ciclo de hábitos de captura da atenção dos titulares para o fornecimento de seus dados – devem ser analisadas partindo-se da premissa de que há a coleta de **dados sensíveis** dos usuários ou ao menos a **inferência de informações sensíveis** a respeito destes.

Tal afirmação se dá porquanto, para que haja a possibilidade de se averiguar, através do processamento algorítmico, informações precisas acerca do comportamento que se quer estimular e das recompensas que se quer reforçar nos usuários, muitas vezes plataformas digitais e *big techs* recorrem a dados de natureza sensíveis para manipular o engajamento dos indivíduos em seus produtos e serviços.

Nesse sentido, mesmo em casos em que já se configura uma prática sub-reptícia por não haver uma coleta através de um consentimento explícito (**art. 7º, IX, do MCI**) ou específico e destacado (**art. 11, I, da LGPD**) de dados sensíveis, podem ainda ocorrer outras ilicitudes pelo cruzamento de dados pessoais não sensíveis disponibilizados pelos titulares, cujas finalidades não haviam sido delimitadas e informadas (**arts. 6º, I e II; 9º, I, da LGPD; e 7º, VIII, do MCI**) anteriormente para um possível uso secundário de "recompensas variáveis" em uma *timeline* de uma mídia social, por exemplo.

Todo esse sistema cíclico de manipulação, fomentado pela última etapa do modelo do gancho – caracterizado pelo **investimento** das próprias empresas de tecnologia em aprimorar os mecanismos persuasivos –, corroboram com uma **violação massiva** do direito fundamental à **proteção de dados pessoais** – preconizado pela **Constituição Federal (CF) em seu artigo**

5º, inciso LXXIX –, bem como tolhe os cidadãos do livre exercício de seu direito à **autodeterminação informativa (art. 2º, II, da LGPD)** e à **privacidade (art. 5º, X, da CF)** – ainda mais ao considerarmos as implicações relativas aos dados e às inferências de informações sensíveis.

A capacidade de explorar a vulnerabilidade cognitiva e emocional a partir da matriz captológica da Economia Psíquica dos Algoritmos, todavia, não é a única forma de manipular comportamentos, muito menos constitui o método mais invasivo para inferir dados sensíveis de titulares. Após a esquematização de violações referentes à captologia, analisaremos como se dá a ilicitude da manipulação mediante a matriz preditiva.

Tabela 3 – Violações jurídicas – Captologia Comportamental

MATRIZ CAPTOLÓGICA		
LGPD	**CDC**	**CF**
Art. 5º, XII (consentimento livre, inequívoco e específico)	Art. 6º, II e III (liberdade de escolha e igualdade nas contratações; informações adequadas e corretas em relação ao preço dos produtos e serviços ofertados)	Art. 5º, LXXIX (direito à proteção de dados pessoais)
Art. 6º, I, II e III (princípios da finalidade, adequação e necessidade)	Art. 4º, III (harmonização dos interesses das partes com base na boa-fé e no equilíbrio da relação de consumo)	Art. 5º, X (vida privada, intimidade - privacidade)
	Guidelines nº 5 EDPB	**MCI**

Art. 9º, *caput* (dever de prestar informação clara, adequada e ostensiva) + rol exemplificativo	Granularidade do consentimento (vedação a "empacotamento e amarração")	Art. 7º, VIII (finalidades determinadas e lícitas)
Art. 9º, I (dever de informação relativo às finalidades do tratamento)		Art. 7º, IX (consentimento explícito)
Art. 8º, §5º (revogação do consentimento facilitada, acessível e gratuita)		
Art. 8º, §3º (vício de consentimento)		
Art. 11, I (consentimento específico e destacado)		
Art. 2º, II (direito à autodeterminação informativa)		

5.2.2 – Práticas sub-reptícias da predição comportamental

A matriz preditiva da Economia Psíquica dos Algoritmos confere às empresas de tecnologia a capacidade de extração de dados pessoais sensíveis a partir do reconhecimento de expressões faciais e da sua matematização, de modo a possibilitar a predição comportamental de seus consumidores. Ao utilizarem-se da **psicometria** e do ***profiling*** (vide item 3.2.2), as inferências algorítmicas ultrapassam meras previsões comportamentais e passam a constatar características personalíssimas dos indivíduos.

Diante disso, em casos como os de ***marketing* direcionado**[322] mencionados no item 3.2.2, em que o titular **não mantenha relação pré-estabelecida**[323] com o fornecedor de produtos e serviços, os anúncios publicitários são adaptados a cada um através do uso de técnicas de ***microtargeting*** e **perfilização**. Justamente pela inexistência de relação prévia entre as partes envolvidas, os agentes de tratamento não poderiam se utilizar da base legal do legítimo interesse para tratar tais dados pessoais, sob eventual justificativa de impossibilidade de coleta de consentimento dos titulares.

Nessa senda, ao não coletarem o **consentimento específico** dos usuários para o tratamento de **dados sensíveis**, nem **granularizar** a anuência para as respectivas finalidades de publicidade targetizada e outros **propósitos específicos**, as plataformas digitais e *big techs* que se utilizam desta modalidade de *profiling* violam os **artigos 11, I; 5º, XII; e 9º, I, da LGPD, bem como o artigo 7º, VIII, do MCI**. Tais violações decorrem do fato de que as empresas de tecnologia, como controladoras de dados pessoais, além de possuírem o dever de coletar o consentimento nos termos das legislações vigentes, devem também garantir a informação relativa às finalidades de tratamento aos titulares.

Ademais, cabe ressaltar que, sem prestar as **informações claras, adequadas e ostensivas relativas às finalidades** do tratamento (**arts. 6º, I; e art. 9º, *caput*, da LGPD**), o **titular pode ser levado a erro ou submetido a discriminações** por parte de anúncios publicitários de produtos ou serviços oferecidos por meio da plataforma, mídia social ou aplicativo pelos quais estejam sendo veiculados. Tal situação pode repercutir em **publicidade enganosa e abusiva**, cujas práticas são vedadas pelo Código de Defesa do Consumidor (**art. 37, §§1º, 2º e 3º, do CDC**).

Como usualmente as práticas de targetização publicitária e *marketing* direcionado ocorrem de maneira recorrente e a uma coletividade de consumidores e titulares de dados, há de se considerar um claro **risco a seus direitos à proteção de dados pessoais (art. 5º, LXXIX, da CF), autodeterminação informativa (art. 2º, II, da LGPD) e à privacidade (art. 5º, X, da CF)** – à semelhança das ameaças trazidas pela captologia comportamental. Tais riscos

[322] Essa modalidade pode ser realizada por meio do *marketing* indireto ou *targeted advertisement*, em que diversos atores trocam dados pessoais de titulares entre si para exibirem anúncios em diferentes plataformas. Ainda, cabe ressaltar que geralmente esse cruzamento de dados é relativo a diferentes contextos de monitoramento da vida *online* dos indivíduos. *Cf.*: BIONI. *Op cit.*, 2023, p. 165.

[323] A relação pré-estabelecida entre fornecedor e consumidor é fundamental para caracterizar a legítima expectativa de um controlador de dados para a viabilidade da utilização da base legal do legítimo interesse – *Ibid.*, pp. 164-165.

decorrem do próprio viés manipulatório das práticas da matriz preditiva, que tolhem *per se* a possibilidade de manifestação de vontade livre e inequívoca dos indivíduos, bem como de sua capacidade de inferência de características personalíssimas através do processamento de seus dados sensíveis.

Vale ainda pontuar que os mencionados *softwares* de análise de emoções desta matriz da Economia Psíquica dos Algoritmos (vide item 3.2.2), ao coletarem dados biométricos de expressões faciais sem o **consentimento expresso** do titular, **violam** não apenas a sua **livre, inequívoca, informada e específica manifestação de vontade (art. 5º, XII, LGPD)** diante de tal extração de dados sensíveis; mas também constituem uma afronta ao princípio basilar da **boa-fé** – que alicerça tanto as relações entre **agentes de tratamento e titulares (art. 6º, *caput*, da LGPD)**, quanto **entre fornecedores e consumidores (art. 4º, III, do CDC).**

Todavia, mesmo se porventura os titulares manifestarem seu consentimento específico e destacado para finalidades determinadas e granularmente dispostas, a fim de que sejam suas expressões faciais matematizadas e codificadas por técnicas de psicometria e análise algorítmica, deve ser questionada **quão inequívoca** foi a sua anuência. Isso porque, como já discorrido, todos os pressupostos de assimetria informacional, vieses manipulatórios e influências de emoções nos processos decisórios não podem ser descartados quando as **poucas opções de inserção e inclusão social no mundo digitalizado** utilizam-se de mecanismos de persuasão comportamental contra seus usuários e consumidores.

Tendo isso em mente, após a tabela de ilícitos constatados da matriz preditiva da Economia Psíquica dos Algoritmos, passaremos à análise das violações praticadas pelas companhias de tecnologia por meio de pesquisas de *neuromarketing*, cujo advento permitiu um nível de intrusividade ainda maior no entendimento e, por conseguinte, na manipulação da tomada de decisão dos indivíduos.

Tabela 4 – Violações Jurídicas – Predição Comportamental

MATRIZ PREDITIVA		
LGPD	**CDC**	**CF**
Art. 5º, XII (consentimento livre, inequívoco e específico)	Art. 37, §§1º, 2º e 3º (vedação à publicidade enganosa e abusiva)	Art. 5º, LXXIX (direito à proteção de dados pessoais)
Art. 6º, *caput* (princípio da boa-fé)	Art. 4º, III (harmonização dos interesses das partes com base na boa-fé e no equilíbrio da relação de consumo)	Art. 5º, X (vida privada, intimidade - privacidade)
Art. 6º, I (princípio da finalidade)		**MCI** Art. 7º, VIII (finalidades determinadas e lícitas)
Art. 9º, *caput* (dever de prestar informação clara, adequada e ostensiva)		Art. 7º, IX (consentimento explícito)
Art. 9º, I (dever de informação relativo às finalidades do tratamento)		
Art. 11, I (consentimento específico e destacado)		

Art. 2º, II (direito à autodeterminação informativa)		

5.3 – A ilicitude de pesquisas de *neuromarketing*

O subcapítulo 3.3 da seção I apresentou que a Neurociência hoje já comprova que os processos decisórios de compra possuem influência determinante do inconsciente e das emoções. Diante disso, os estudos de *neuromarketing* partem dessa premissa para coletar dados pessoais ainda mais apurados, geralmente relativos a processos fisiológicos e cognitivos dos indivíduos, a fim de fomentarem a manipulação comportamental de usuários e consumidores de plataformas digitais, *big techs* e demais companhias vigilantes.

As pesquisas desse campo – que, para fins deste trabalho, serão analisadas aquelas desenvolvidas pelas próprias empresas de tecnologia[324] – constituem métodos invasivos sob o ponto de vista psicojurídico, tanto por alentarem estímulos inconscientes visando à persuasão do comportamento humano, quanto por repercutirem em violações constitucionais e infraconstitucionais.

Como visto, os experimentos são pautados pela inferência de diversos dados pessoais sensíveis, tais como: atividade metabólica cerebral, função elétrica cerebral, sudorese, fixação do olhar e dilatação da pupila, dentre outras informações referentes à saúde do titular. Esses dados são constatados a partir de diferentes exames; como, por exemplo, a Tomografia de Emissão de Pósitrons, a Imagem por Ressonância Magnética Funcional, o Eletroencefalograma, a Resposta da Condutividade da Pele e o Rastreamento Ocular (vide subcapítulo 3.3).

Com isso, em uma situação em que um titular de dados pessoais se vê diante de uma gama de experimentos invasivos dessas modalidades, o intérprete do direito deve considerar a sua **vulnerabilidade** diante dos contratos – geralmente de adesão – e termos de consentimento que são oferecidos unilateralmente a ele. Deve ser considerado também o fato de que, se houver remuneração pela empresa ao titular em decorrência da pesquisa, tal prestação pecuniária **não**

[324] Não serão analisadas neste trabalho pesquisas desenvolvidas por órgãos de pesquisa que se enquadre no artigo 7º, IV, da LGPD.

transfere à companhia o direito de tratar os dados deste indivíduo como bem entender, mesmo que para fins de pesquisa.

O **direito à proteção de dados pessoais** é um direito fundamental, consagrado expressamente pela Constituição Federal brasileira, fazendo com que as empresas que não realizem o tratamento dos dados pessoais de titulares submetidos às pesquisas de *neuromarketing* de maneira adequada e lícita afrontem diretamente o **artigo 5º, LXXIX, da CF**. Além disso, assim como na Economia Psíquica dos Algoritmos, dessa violação decorrem a não observância do **direito à autodeterminação informativa** (**art. 2º, II, da LGPD**), pela impossibilidade de autonomia em relação ao tratamento de seus dados diante de tais pesquisas; **e à privacidade** (**art. 5º, X, da CF**), em decorrência da inferência de informações personalíssimas – o subcapítulo 3.3 relatou que os experimentos são capazes de constatar preferências de consumidores por produtos, marcas, *design* de embalagens, trailers de filmes, interfaces de sites, dentre outras.

Ainda, no que tange ao debate ético[325] pontuado no subcapítulo 3.3, pode-se afirmar que, quando não coletado o consentimento livre, inequívoco, informado (**art. 5º, XII, da LGPD**) e específico – assim como destacado e explícito (**art. 11, I, da LGPD; e art. 7º, IX, do MCI**) – do titular para as finalidades das pesquisas de *neuromarketing*, o **princípio da dignidade humana**, que tem fundamento constitucional no **art. 1º, III, da CF**, é também violado pelas entidades vigilantes.

Ademais, vale ressaltar que o **consentimento** do titular deve ser fornecido para cada exame realizado, seja por métodos mais ou menos invasivos, de modo que sejam delimitadas de **maneira granularizada** quais as finalidades almejadas por cada um dos respectivos exames, sob risco de violação dos **artigos 6º, I; 9º, *caput* e I, da LGPD; e 7º, VIII, do MCI**; bem como de estarem em dissonância com o estipulado pelas **Guidelines de nº 5 do EDPB**.

Por exemplo, uma *big tech* que deseje realizar testes por **Imagem por Ressonância Magnética Funcional** para mapear zonas de ativação cerebral de titulares, deve informá-los que serão coletados dados pessoais a respeito de seu fluxo sanguíneo e oxigenação do sangue a fim de se constatar alterações causadas por estímulos associados a emoções inconscientes. Deve ainda coletar seu consentimento específico para cada uma das finalidades que desejam alcançar,

[325] Levantado por: FRAZÃO. *Op. cit.*, 2019.

dentre elas: i) testar novos produtos; ii) testar campanhas publicitárias; iii) verificar reações do consumidor a novos preços de produtos e serviços; iv) testar reações de consumidores a novas marcas; v) prever comportamentos (vide Tabela 1).

Da mesma maneira, uma plataforma digital que se utilize de um método menos invasivo, a exemplo do **Rastreamento Ocular**, para medição da fixação do olhar, dos movimentos de procura dos olhos, da dilação da pupila e das piscadas dos seus usuários, tem o dever de informar-lhes que coletam estes dados sensíveis para fins de modulação de atenção, engajamento e memória. Além disso, o consentimento coletado deve ser granularizado para as finalidades almejadas, sendo elas: i) testar novas interfaces de sites; ii) verificar reações de consumidores a compras; iii) testar novos materiais publicitários; iv) testar alocação visual de produtos; v) analisar filtragem de informação por usuários; vi) determinar hierarquia de percepção a estímulos materiais (vide Tabela I).

Caso as informações fornecidas ao consumidor-titular não sejam suficientes para a sua tomada de decisão isenta de manipulação e vício (**art. 8º, §3º, da LGPD**), as empresas que realizam as pesquisas de *neuromarketing*, enquanto fornecedoras e controladores, violam o dever de prestar informações claras, adequadas e ostensivas (**art. 9º, *caput*, da LGPD; art. 6º, III, do CDC)**, bem como agem de má-fé (**art. 6º, *caput*, da LGPD; e art. 4º, III, do CDC**) ao omitirem informação essencial ou ao submeterem seus usuários à sobrecarga de informações, de maneira a levarem-nos a erro.

Diante do exposto, após a análise de práticas sub-reptícias empregadas por, em sua maioria – porém não se resumindo a –, plataformas digitais e *big techs*, resta discorrer a respeito de casos trazidos no subcapítulo 2.2 deste trabalho. Após a tabela de possíveis ilicitudes constatadas pelas pesquisas de *neuromarketing*, serão abordadas violações de consentimentos praticadas por empresas de outros setores econômicos.

Tabela 5 – Violações Jurídicas – Pesquisas de *neuromarketing*

<table>
<tr><th colspan="3">NEUROMARKETING</th></tr>
<tr><th>LGPD</th><th>CDC</th><th>CF</th></tr>
<tr><td>Art. 5º, XII (consentimento livre, inequívoco e específico)</td><td>Art. 6º, III (dever de prestar informações adequadas e corretas ao consumidor)</td><td>Art. 5º, LXXIX (direito à proteção de dados pessoais)</td></tr>
<tr><td>Art. 6º, caput (princípio da boa-fé)</td><td>Art. 4º, III (harmonização dos interesses das partes com base na boa-fé e no equilíbrio da relação de consumo)</td><td>Art. 5º, X (vida privada, intimidade - privacidade)</td></tr>
<tr><td>Art. 6º, I (princípio da finalidade)</td><td>Guidelines nº 5 EDPB</td><td>Art. 2º, III (princípio da dignidade humana)</td></tr>
<tr><td rowspan="2">Art. 9º, caput (dever de prestar informação clara, adequada e ostensiva)</td><td rowspan="2">Granularidade do consentimento (como garantia da delimitação e informação adequada das finalidades almejadas pelo tratamento)</td><td>MCI</td></tr>
<tr><td>Art. 7º, VIII (finalidades determinadas e lícitas)</td></tr>
<tr><td>Art. 9º, I (dever de informação relativo às finalidades do tratamento)</td><td></td><td>Art. 7º, IX (consentimento explícito)</td></tr>
<tr><td>Art. 8º, §3º (vício de consentimento)</td><td></td><td></td></tr>
<tr><td>Art. 11, I (consentimento específico e destacado)</td><td></td><td></td></tr>
</table>

Art. 2º, II (direito à autodeterminação informativa)		

5.4 – Violações de outros setores econômicos: empresas varejistas e birôs de crédito

No final do capítulo 2, foram mencionados dois casos de companhias do setor de varejo e um de birôs de crédito que se utilizam de mecanismos ilícitos de extração de dados pessoais de titulares. Sob a justificativa genérica de otimização de seus serviços, essas entidades privadas praticam diversas violações aos direitos de consumidores-titulares que merecem destaque neste trabalho, ainda mais ao considerarmos as ameaças de sua arquitetura manipulatória que repercutem muitas vezes em uma violação do **princípio da não discriminação (art. 6º, IX, da LGPD)**, como se verá adiante.

O primeiro caso é o de empresas que empregam técnicas de modelagem e análise de dados para realizar ***marketing*** **direcionado abusivo** a consumidores a partir da inferência de dados sensíveis, a exemplo do caso Target[326] (vide subcapítulo 2.2). Como, nesta situação específica, consumidor e fornecedor já mantinham vínculo e, portanto, o controlador possui – em um primeiro momento – interesse legítimo para a targetização publicitária, é possível afirmar que a base legal para o tratamento desta modalidade é a do **legítimo interesse**, e não a do consentimento. Entretanto, ao considerarmos que foram constatadas informações sensíveis – no caso Target, em relação à gravidez de clientes antes mesmo que as famílias destas soubessem – para a inferência e divulgação de informações de cunho personalíssimo, a legitimidade das finalidades propostas é posta em xeque.

Isso porque a primeira fase do teste de balanceamento do legítimo interesse considera, a partir da situação concreta, se as finalidades almejadas pelo controlador são legítimas (**art. 10, *caput* e I, da LGPD**), devendo os agentes de tratamento priorizarem a necessidade (**art. 10, §1º, da LGPD**) dos dados tratados e as salvaguardas aos direitos dos titulares que possam ser impactados pelo processamento (**art. 10, II, da LGPD**). Como, no caso em análise, não houve a observância de nenhum desses parâmetros, além de discriminar os consumidores-titulares (**art. 6º, IX, da LGPD**), essas empresas podem praticar publicidade abusiva (**art. 37, *caput* e**

[326] Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4ccdae5b6668>. Acesso em 12 dez. 2022.

§2º, do CDC) – dependendo dos dados sensíveis inferidos, por serem capazes de veicularem, de maneira direcionada, conteúdos que explorem o medo, incitem violência ou se aproveitem da deficiência de julgamento do consumidor.

Em contrapartida, no que concerne ao segundo caso, trata-se de companhias que coletam dados sensíveis de expressões faciais de consumidores que adentram lojas físicas através de tecnologia de reconhecimento facial, sem o seu consentimento (**art. 7º, I, da LGPD**), para a finalidade de traçar perfis de consumo (vide caso Hering no subcapítulo 2.2). Além de não informarem seus consumidores sobre o uso de tais tecnologias, violando o seu dever de informação como controladoras e fornecedoras de serviços (**art. 9º, *caput*, da LGPD; e art. 6º, III, do CDC**), tais empresas – diferentemente das anteriores – não podem se valer da base legal do legítimo interesse por já se proporem a atingir finalidades de *profiling* passíveis de resultar em condutas discriminatórias aos consumidores (**art. 6º, IX, da LGPD**) – além de não estabelecerem a análise dos dados para fins de *marketing* direto, e sim para manipulação do consumidor no local de compra.

Logo, além de se aproveitarem da vulnerabilidade de seus consumidores (**art. 4º, I, do CDC**), as empresas que não informam os titulares de dados sobre o uso das tecnologias de reconhecimento facial para a finalidade de perfilização comportamental tolhem a liberdade destes de consentir livre, inequívoca, informada (**art. 5º, XII, da LGPD**) e especificamente (**art. 11, I, da LGPD**) para o tratamento de seus dados pessoais sensíveis e põem em risco, por conseguinte, a sua autodeterminação sobre a circulação de seus dados (**art. 2º, II, da LGPD**).

Por fim, vale ressaltar o terceiro caso mencionado no subcapítulo 2.2, que se refere à utilização de técnicas de *profiling* por birôs de crédito a partir de bases de dados enviesadas e de dados sensíveis. Como já visto no subcapítulo 4.4, a prática de *credit scoring* é lícita no Brasil – respeitados os artigos 5º, inciso IV, e 7º, inciso I, da Lei nº 12.414/2011, e de acordo com o que foi firmado pela jurisprudência do STJ –, **desde que não haja o processamento de informações excessivas** pelas entidades avaliadoras de crédito.[327] Assim, a partir do momento em que birôs de crédito tratam dados pessoais sensíveis de titulares – tais como aqueles de origem racial, étnica, convicção religiosa, cunho político, dados de saúde, dados genéticos e biométricos – ou dados pessoais que, se advindos de uma base enviesada, pelo seu cruzamento,

[327] Tais entidades se valem da base legal de proteção ao crédito (art. 7º, X, da LGPD) para a prática de *credit scoring.*

podem resultar em informações sensíveis; essas entidades **violam os princípios da não discriminação, necessidade e finalidade** (**art. 6º, IX, III e I, da LGPD**).

Caso venham ainda a negar o acesso dos titulares às informações sobre eles contidas em seus bancos de dados, além de afrontarem o **artigo 9º da LGPD**, vão de encontro com os **princípios do livre acesso e da transparência (art. 6º, IV e VI, da LGPD**), bem como violam **o artigo 5º, II, da Lei do Cadastro Positivo (LCP)**.[328] Além do dever de informação, cabe pontuar que, apesar de não se basear na coleta do consentimento para tratar os dados a fim de realizar a análise do crédito, insta salientar que constitui um direito do titular optar por encerrar ou cancelar o cadastro (**art. 5º, I, da LCP**), constituindo uma manifestação de vontade por mecanismo *opt-out*, cuja inobservância incorre na violação do **artigo 5º, §6º, I, da LCP**.

Portanto, ao analisarmos os casos do subcapítulo 2.2, torna-se possível concluir que as condutas ilícitas de cunho manipulatório contra titulares de dados não são exclusivas de plataformas digitais e *big techs*. A fim de que possamos melhor compreender o que foi abordado neste subcapítulo, a seguir, segue tabela das principais violações jurídicas constatadas por empresas de outros setores econômicos.

Tabela 6 – Violações Jurídicas – Varejistas e birôs de crédito

EMPRESAS VAREJISTAS E BIRÔS DE CRÉDITO		
LGPD	**CDC**	**LCP**
Art. 6º, IX, III e I (princípios da não discriminação, necessidade e finalidade)	Art. 6º, III (dever de prestar informações adequadas e corretas ao consumidor)	Art. 5º, II (acesso gratuito a informações, independente de justificativa)

[328] "Art. 5º São direitos do cadastrado:
II - **acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados**, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;" (grifos nossos) – BRASIL. *Lei 12.414, de 09 de junho de 2011*. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, Brasília, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 20 dez. 2022.

Art. 10, *caput* e I (finalidades almejadas pelo controlador devem ser legítimas)	Art. 37, *caput* e §2º (vedação à publicidade abusiva)	Art. 5º, I (direito ao cancelamento de cadastro)
Art. 10, §1º (ao utilizar-se do legítimo interesse, deve ser observado o princípio da necessidade)	Art. 4º, I (reconhecimento da vulnerabilidade do consumidor)	Art. 5º, §6º, I (dever de cancelamento pelo gestor após solicitação do cadastrado)
Art. 10, II (balanceamento de salvaguardas)		
Art. 9º, *caput* (dever de prestar informação clara, adequada e ostensiva)		
Art. 7º, I (base legal do consentimento)		
Art. 5º, XII (consentimento livre, inequívoco e específico)		
Art. 11, I (consentimento específico e destacado)		
Art. 2º, II (direito à autodeterminação informativa)		
Art. 6º, IV e VI (princípios do livre acesso e da transparência)		

Em suma, são diversas as práticas sub-reptícias constatadas por entidades privadas no capitalismo de vigilância, tanto do setor tecnológico, quanto de outras searas econômicas. O aprimoramento das técnicas manipulatórias de titulares de dados, comprovado pela Economia Comportamental, Economia Psíquica dos Algoritmos e Neurociência, demonstra o quão desafiador é – para o intérprete do direito – dimensionar a adjetivação estipulada pela LGPD ao consentimento. Assim como, em um diálogo de fontes, torna-se de extrema relevância a coadunação de princípios e parâmetros estabelecidos por normas que protejam o titular em sua posição de vulnerabilidade diante do poder de manipulação de plataformas digitais, *big techs* e outras companhias que porventura processem seus dados pessoais.

Todavia, a partir da exposição feita nos capítulos 4 e 5 deste trabalho, nota-se gradualmente que a **visão por parte de entidades privadas vigilantes do titular-consumidor enquanto mero expectador passivo ou simplesmente cobaia de testes experimentais** propriamente ditos **não condiz** com a **perspectiva de incentivo ao empoderamento e autodeterminação informacional trazida pelo ordenamento jurídico pátrio**. Importa ressaltar, portanto, que há uma **divergência na óptica que "psico-orienta"** as ideias de concepção de indivíduo para os atores envolvidos, de um lado na manipulação e, de outro, no dever de garantia de seus direitos.

Tal **visão humanista do indivíduo** é importante para a compreensão do próximo capítulo, como restará claro a seguir, visto que abordará as medidas de *accountability*, *enforcement* e salvaguardas necessárias por parte dos atores capazes de balancear a dupla função de normas de proteção de dados pessoais, bem como versará a respeito de mecanismos de contravigilância dos quais titulares podem fazer uso a fim de se estabelecer uma mínima simetria informacional entre vigilantes e vigiados.

CAPÍTULO 6 – Propostas de reforço de salvaguardas e contravigilância

Antes de adentrarmos nas medidas de *accountability* e *enforcement* capazes de proverem os titulares com salvaguardas aos seus direitos, bem como nas estratégias de contravigilância que estes podem adotar como vigiados em um sistema vigilante, é importante esmiuçar o entendimento "psico-orientativo" que o ordenamento jurídico dá ao cidadão enquanto ser humano.

Tal como mencionado no final do capítulo anterior, o **direito à proteção de dados pessoais** aborda psicologicamente a concepção do indivíduo **sob um prisma humanista**, isto é, a partir da valorização da capacidade do ser humano de ter **consciência sobre suas escolhas**. Isso porque o arcabouço jurídico brasileiro confere aos cidadãos tanto a **autodeterminação** sobre suas características personalíssimas, quanto a **proteção do seu poder decisório** (vide legislação do capítulo 4), levando ao entendimento de que é um pressuposto essencial para o ordenamento jurídico a **garantia do livre arbítrio em uma ordem constitucional democrática**.

A Psicologia Humanista surgiu oficialmente durante a década de 1960[329] nos Estados Unidos e tem como seus maiores expoentes Abraham Maslow, Gardner Murphy, Gordon Allport e Carl Rogers. Ademais, nasceu em meio a um movimento de contracultura em **oposição às teorias behavioristas,** dentre outras notadamente deterministas, que predominavam à época, por priorizar o ser humano diante de suas potencialidades e atuações frente a adversidades.[330]

Não é por outro motivo que há um evidente **conflito** entre a **óptica behaviorista experimental** pela qual as **empresas de tecnologia** veem os seus consumidores **e as lentes** utilizadas pelo **ordenamento jurídico** para dar foco aos titulares. Enquanto as primeiras os colocam em uma posição de **espectadores facilmente passíveis de manipulação**; o segundo,

[329] Especificamente no ano de 1962. – RIVEROS AEDO, Edgardo. *La psicología humanista*: sus orígenes y su significado en el mundo de la psicoterapia a medio siglo de existência. Ajayu, Órgano de Difusión Científica del Departamento de Psicología de la Universidad Católica Boliviana San Pablo, v. 12, n. 2, pp. 135- 186, 2014, p. 138.

[330] A teoria desenvolvida por Maslow, por exemplo, que é considerado "o pai da Psicologia Humanista", tem como ponto central o estudo voltado para o potencial humano de "autorrealização", que seria a busca pelo atingimento de todas as suas plenas potencialidades enquanto ser humano, incluindo a superação de adversidades divididas em etapas de prioridades – daí adveio, inclusive, a Teoria da Hierarquia das Necessidades Humanas. – *Cf.*: RIVEROS AEDO. *Op. cit.*, 2014, pp. 145-147; e SOUZA, Cid Marconi Gurgel de; CARRÁ, Bruno Leonardo Câmara. A hierarquia das necessidades de Maslow e os danos extrapatrimoniais: um paralelo entre o Direito e a Psicologia Humanista. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 59, n. 234, pp. 11-33, 2022, pp. 15-18.

ainda que considere a vulnerabilidade flagrante dos titulares enquanto uma evidência da **falácia de sua soberania**[331]-[332] no contexto datificado atual, **faz tal consideração por ponderar a necessidade de garantir-lhes a autodeterminação em seus processos decisórios**.

Diante disso, torna-se possível justificar por que, em uma economia fomentada pela persuasão e processos cíclicos de investimentos em práticas manipulativas para a extração ilícita de dados pessoais, deve ser priorizada uma **abordagem pró-humanismo** por parte do intérprete do direito, de maneira a **valorizar as potencialidades dos cidadãos preconizadas pela legislação constitucional e infraconstitucional**. Nesse sentido, este capítulo se propõe a trazer medidas de proteção aplicáveis por autoridades e mecanismos de engajamento práticos ao consumidor-titular capazes de conferir-lhe, ao menos em certa medida, maior autodeterminação e livre arbítrio em seus processos decisórios.

6.1 – Medidas de *accountability* e *enforcement:* ANPD e Senacon como atores centrais de uma governança multissetorial

A partir da concepção da tutela jurídica aos titulares enquanto um pressuposto de garantia de suas potencialidades nos processos decisórios relativos ao fluxo de seus dados pessoais, abrem-se leques de oportunidades para que se revertam as situações de manipulação às quais estão submetidos no capitalismo de vigilância.

---

[331] A nomenclatura "falácia da soberania do consumidor" é utilizada por Ana Frazão para se referir à **vulnerabilidade** à qual os consumidores estão submetidos em meio à economia digital. – *Cf.*: FRAZÃO. *Op. cit.*, 2021. Segundo Frazão, a própria ideia de soberania do consumidor foi ancorada em **preceitos idealizados** que funcionariam muito bem em situações teóricas, porém não práticas, como a "liberdade do consumidor, racionalidade do consumidor, acesso à informação, mercados competitivos e ausência de custos de troca ou migração (os chamados *switching costs*)". Para uma efetiva e concreta soberania do consumidor-titular, todos esses pressupostos do mercado devem estar presentes, enquanto, na realidade, é raro encontrar a presença de ao menos um deles nas relações de consumo. – *Cf.*: FRAZÃO, Ana. *O mito da soberania do consumidor*. É legítimo esperar que as soluções de mercado protejam o consumidor?, Jota, publicado em 01 dez. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-mito-da-soberania-do-consumidor-01122021>. Acesso em: 08 jan. 2023.

[332] Ainda sobre a falácia da soberania do consumidor, importa destacar que John Kenneth Galbraith demonstra que essa premissa, muito utilizada pela economia tradicional, faz com que **a ciência econômica deixe de explicar os problemas e passe a tirar conclusões precipitadas sob a perspectiva social.** O pressuposto de soberania mascara, portanto, uma série de fatores conflituosos entre consumidores e empresas, "enquanto o afastamento de tal premissa põe luz sobre as desarmonias do mundo real e a necessidade de resolver tais conflitos". – FRAZÃO, Ana. *Economia como um sistema de crenças*. Entendendo os bastidores do debate econômico a partir da obra de John Kenneth Galbraith, Jota, publicado em 14 dez. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/economia-como-um-sistema-de-crencas-14122022>. Acesso em 08 jan. 2023.

Isso porque torna-se possível estabelecer parâmetros de reforços de salvaguardas que fomentem a autonomia e o engajamento dos cidadãos por parte de atores do setor público, que, por sua vez, têm o dever de tutelar os direitos de titulares de dados e consumidores. Assim como é cabível a aplicação de medidas que incrementem a prestação de contas a esses atores por parte das entidades privadas vigilantes, de modo a garantir transparência e convergência – ou comprovar divergência, nos casos apresentados – com a legislação de proteção de dados e consumerista.

Dessarte, considerando a **governança multissetorial** brasileira hoje existente no campo da proteção de dados pessoais – isto é, um **conjunto de diferentes atores** que, envolvidos em meio a **negociações**, buscam **garantir o adequado fluxo de dados pessoais**, bem como o próprio **direito à sua proteção**[333] – nota-se uma necessidade de atuação conjunta de órgãos regulatórios a fim de **promover medidas de *accountability*** – que visem à comprovação de condutas ilícitas –, bem como com o objetivo de **exercer mecanismos de *enforcement*** mais eficazes – que possibilitem a responsabilização por aqueles que violem a legislação.

Com isso, importa destacar que a **Autoridade Nacional de Proteção de Dados (ANPD)**, como autarquia federal dotada de autonomia técnica para a defesa dos direitos dos titulares de dados[334] – e a **Secretaria Nacional do Consumidor (Senacon)** – enquanto órgão vinculado ao Ministério da Justiça responsável pela defesa das salvaguardas dos consumidores[335] – têm especial relevância neste cenário. Tanto a ANPD, quanto a Senacon possuem a legitimidade de intervir, em um sistema de regulação que envolve múltiplos atores, em situações em que forem constatadas ameaças ou comprovações de violação a direitos no

[333] O conceito e a definição de **governança multissetorial** foram extraídos da obra *Regulação e Proteção de Dados Pessoais*: *O Princípio da Accountability*, de Bruno Bioni (Vide Capítulo 5: O caso do Combate ao Spam: Da Formação do Fórum Público ao Processo de Deliberação das Contas Prestadas). *Cf.*: BIONI. *Op. cit.*, 2022.

[334] "Art. 1º A Autoridade Nacional de Proteção de Dados - ANPD, órgão integrante da Presidência da República criada pela Lei nº 13.709, de 14 de agosto de 2018, dotada de autonomia técnica e decisória, com jurisdição no território nacional e com sede e foro no Distrito Federal, tem por finalidade proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural." – ANPD. Autoridade Nacional de Proteção de Dados, *Portaria nº 1, de 08 de março de 2021*. Estabelece o Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-1-de-8-de-marco-de-2021-307463618>. Acesso em 10. dez. 2022.

[335] "Art. 1º - A Secretaria Nacional do Consumidor - Senacon, órgão específico singular, integrante da Estrutura Regimental do Ministério da Justiça e Segurança Pública, a que se refere o art. 2º, inciso II, alínea "c", do Anexo I do Decreto nº 9.150, de 4 de setembro de 2017, tem por finalidade exercer as competências estabelecidas na Lei nº 8.078, de 1990, na Lei nº 9.008, de 1995, [...]" – SENACON. Secretaria Nacional do Consumidor, *Portaria nº 905, de 24 de outubro de 2017*. Aprova o Regimento Interno da Secretaria Nacional do Consumidor.Disponível em: <https://www.gov.br/mj/pt-br/acesso-a-informacao/institucional/sumario/regimento/senacon/regimento-senacon-portaria-905-2017.pdf>. Acesso em: 22 dez. 2022.

processo de tomada de decisão livre, consciente e inequívoca – bem como específica – de titulares e consumidores.

Logo, no que tange a medidas de *accountability*, quando houver suspeita ou provas de que uma plataforma digital ou *big tech* estiver praticando uma das técnicas manipulatórias abordadas no capítulo 3 deste trabalho, a ANPD poderá determinar a elaboração e submissão de **relatório de impacto à proteção de dados pessoais (RIPD**),[336] especificando os tipos de dados coletados – inclusive os sensíveis –, bem como a metodologia de coleta – para averiguar a existência de práticas manipulativas ou não – e as medidas de salvaguardas e mitigação de riscos que foram adotadas – se existentes.[337] Esses requisitos estipulados pelo parágrafo único do artigo 38 da LGPD não constituem rol taxativo, fazendo com que outras hipóteses possam ser exigidas pela Autoridade, com fins de que seja pormenorizada a existência de persuasão do titular.

Por exemplo, a ANPD poderia, dentro dos limites estabelecidos à observância do segredo industrial e comercial, demandar, em casos de *marketing* direcionado, a **comprovação de relação consumerista prévia** entre fornecedor e consumidor para averiguar qual base legal o tratamento deveria se apoiar e se foi adotada dentro das regras preconizadas pela LGPD. Assim como, nos casos de pesquisas de *neuromarketing*, avaliar a necessidade de **envio das diretrizes éticas** parametrizadas pelas empresas realizadoras de experimentos, de modo a melhor averiguar se os direitos fundamentais dos titulares foram considerados nas referidas pesquisas.

A Senacon, em complemento, ao evidenciar práticas sub-reptícias à livre manifestação volitiva dos consumidores por vias manipulativas, tem a viabilidade de expedir notificações às empresas a fim de que prestem informações[338] sobre danos causados ou risco de dano ao consumidor. A Secretaria Nacional do Consumidor pode exigir que sejam **esclarecidos e corrigidos termos de uso e políticas de privacidade opacos ou que contenham sobrecarga**

---

[336] Vide: Art. 38, *caput*, da LGPD transcrito abaixo.

[337] "Art. 38. A autoridade nacional **poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis**, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, **no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta** e para a garantia da segurança das informações e a análise do controlador com relação a **medidas, salvaguardas e mecanismos de mitigação de risco adotados**." (grifos nossos) – BRASIL. *Op. cit*., 2018.

[338] Vide: Art. 55, §4º, do CDC: "§ 4° Os órgãos oficiais poderão expedir notificações aos fornecedores para que, sob pena de desobediência, prestem informações sobre questões de interesse do consumidor, resguardado o segredo industrial." – BRASIL. *Op. cit*., 1990.

informacional que levem o consumidor-titular a vício de consentimento, por exemplo. Tal como, em casos de publicidade enganosa ou abusiva por *marketing* direto, pode demandar a **correção das informações** veiculadas ao consumidor **por meio de uma plataforma em relação ao serviço ou produto publicizado ou impor a divulgação de contrapropaganda**.[339]

Em relação a mecanismos de *enforcement*, vale ressaltar que ambos os atores, ANPD e Senacon, possuem competência para a **aplicação de medidas *ex post* e *ex ante,*** isto é, reativas e preventivas em casos de descumprimento a normas da LGPD e do CDC, respectivamente. Nesse sentido, cabe pontuar que, ao violarem os dispositivos mencionados no capítulo 4 deste trabalho, as entidades privadas que pratiquem manipulação comportamental de titulares podem estar submetidas à aplicação das **sanções** estipuladas nos artigos contidos no Capítulo VIII da LGPD e no Capítulo VII do CDC.

Tais artigos referem-se às sanções administrativas cabíveis mediante constatação de infrações das respectivas leis. As sanções elencadas pelas referidas leis, vale pontuar, não excluem a responsabilização das empresas em outras esferas jurídicas e abarcam diversas modalidades especificadas na **LGPD, no seu artigo 52,[340] e no CDC, em seu artigo 56**.[341]

---

[339] Vide: Art. 60, *caput* e §1º, do CDC.

[340] "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 até a sua regularização;
VI - eliminação dos dados pessoais a que se refere a infração;
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." – BRASIL. *Op. cit*., 2018.

[341] "Art. 56. As infrações das normas de defesa do consumidor ficam sujeitas, conforme o caso, às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas:
I - multa;
II - apreensão do produto;
III - inutilização do produto;
IV - cassação do registro do produto junto ao órgão competente;
V - proibição de fabricação do produto;
VI - suspensão de fornecimento de produtos ou serviço;
VII - suspensão temporária de atividade;
VIII - revogação de concessão ou permissão de uso;
IX - cassação de licença do estabelecimento ou de atividade;
X - interdição, total ou parcial, de estabelecimento, de obra ou de atividade;
XI - intervenção administrativa;

Diversas autoridades de proteção de dados e de defesa do consumidor ao redor do mundo já exercem *enforcement* diligente a fim de aplicar sanções a agentes privados que descumpram suas legislações. Alguns exemplos de aplicação de sanções a entidades privadas por autoridades regulatórias em decorrência da inobservância ou da violação da base legal do consentimento, constituindo medidas regulatórias *ex post*, incluem:

> **1.** A já mencionada a condenação, pela Senacon em 2019, da varejista Hering ao pagamento de multa no valor de R$ 58.767,00, destinada ao Fundo de Defesa de Direitos Difusos (FDDD), pela utilização sub-reptícia de tecnologia de reconhecimento facial.[342] Como visto, além de constatar a coleta de dados biométricos de consumidores sem o seu consentimento prévio pela loja Hering do Shopping Morumbi, em São Paulo, a Senacon averiguou a violação dos direitos à informação e os relativos à personalidade dos titulares que adentravam o local à época dos fatos. Essa condenação tem relevância para a aplicação de medidas de *enforcement* pró-consumidor, porquanto foi a primeira relacionada à utilização indevida de tecnologias de reconhecimento facial no Brasil, sendo um divisor de águas para as que viriam em seguida, tal como a ação contra concessionária da Linha 4 do Metrô de São Paulo.[343]
>
> **2.** Outra condenação que vale ser destacada foi a executada pela CNIL (Comissão Nacional de Informática e de Liberdade),[344] autoridade de proteção de dados pessoais francesa, que, em dezembro de 2022, multou a Microsoft Ireland no valor de 60 milhões de euros por não ter possibilitado aos seus titulares de dados a possibilidade de revogar seu consentimento com a mesma facilitada de fornecê-lo em sua política de *cookies*.[345] Além de esta medida ser importante por reforçar o estipulado nas Guidelines de nº 5 do EDPB, em relação à revogação de consentimento facilitada e sem detrimento, a condenação da *big tech* pela autoridade francesa confere parâmetros à ANPD relativos

---

XII - imposição de contrapropaganda." – BRASIL. *Op. cit*., 1990.

342 *Cf*.: *Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial:* Secretaria Nacional do Consumidor condenou a empresa ao pagamento de multa de R$ 58,7 mil por violações ao CDC. Disponível em: <https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial>. Acesso em 12 dez. 2022.

343 *Cf*.: *Idec vai à Justiça contra coleta de emoções de usuários do metrô de SP*, Idec, publicado em: ago. 2018. Disponível em: <https://idec.org.br/noticia/idec-vai-justica-contra-coleta-de-emocoes-de-usuarios-do-metro-de-sp>. Acesso em 15 jan. 2023.

344 Tradução do francês para o português de "Commission Nationale de l'Informatique et des Libertés".

345 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Cookies:* sanction de 60 millions d'euros à l'encontre de MICROSOFT IRELAND OPERATIONS LIMITED, 22 décembre 2022. Disponível em: <https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-microsoft-ireland-operations-limited>. Acesso em 15 jan. 2023.

ao que deve ser exigido de uma empresa de tecnologia em suas políticas de *cookies* – assim como o que deve ser feito em caso de seu descumprimento, observadas as diferenças procedimentais e legislativas entre os países.

3. Um exemplo ocorrido no Peru, em 2021, consistiu na aplicação pela Autoridade Nacional de Proteção de Dados do país, vinculada ao seu Ministério da Justiça e Direitos Humanos (MINJUSDH),[346] de multas totalizadas no valor de 220 mil pesos ao banco Interbank e à seguradora Oncosalud.[347] Tal sanção foi aplicada em decorrência da transferência de dados pessoais de clientes da entidade financeira a uma central de telemarketing para que esta pudesse realizar ligações para os titulares alvos, a fim de que recebessem ofertas de seguros de vida, relacionados a coberturas por acometimentos de câncer, oferecidos pela seguradora. A autoridade peruana entendeu pela responsabilidade solidária de ambas as entidades; no caso do Interbank, por ter compartilhado os dados pessoais dos titulares sem a sua anuência e, no caso da Oncosalud, por não ter coletado o consentimento dos titulares para fins de marketing direcionado.[348] Esse entendimento dado pela autoridade peruana ao caso torna-se relevante para a compreensão de que mais de uma entidade privada pode ser responsabilizada administrativamente, dependendo de sua configuração na cadeia de tratamento, como violadora do consentimento de titulares, restando à ANPD e à Senacon verificar, caso a caso, se houve ou não tal violação pelos agentes.

4. Outro exemplo de 2021, que também teve como pano de fundo o América do Sul, foi a multa aplicada à empresa Rappi pela Superintendência de Indústria e Comércio (SIC) colombiana – correspondente ao CADE[349] brasileiro – em decorrência de solicitação de

---

[346] No espanhol, Autoridad Nacional de Protección de Datos Personales (ANPD) del Ministerio de Justicia y Derechos Humanos (MINJUSDH).

[347] *Cf*.: *Autoridad Nacional de Protección de Datos Personales multa a financiera y a aseguradora oncológica por llamadas sin consentimento*, Gob.pe, publicado em: 14 dez. 2021. Disponível em: <https://www.gob.pe/institucion/minjus/noticias/569980-autoridad-nacional-de-proteccion-de-datos-personales-multa-a-financiera-y-a-aseguradora-oncologica-por-llamadas-sin-consentimiento>. Acesso em 15 jan. 2023.

[348] Na legislação peruana, a utilização de dados pessoais para fins de marketing deve ter consentimento livre, prévio, expresso e informado. – *Cf*.: *Seguradora e financiadora utilizam, sem autorização, dados pessoais para telemarketing publicitário*, Construindo Pontes, 2021. Disponível em: <https://construindopontes.org.br/casos/seguradora-e-financiadora-utilizam-sem-autorizacao-dados-pessoais-para-telemarketing-publicitario/>. Acesso em 15 jan. 2023.

[349] O Conselho Administrativo de Defesa da Concorrência é a autarquia federal responsável pelas investigações, prevenções e repreensão de infrações contra a ordem econômica no Brasil. – *Cf*.: CONSELHO ADMINISTRATIVO DE DEFESA DA CONCORRÊNCIA. Cartilha do CADE, Atualização: maio de 2016. Disponível em: <https://cdn.cade.gov.br/Portal/acesso-a-informacao/perguntas-frequentes/cartilha-do-cade.pdf>. Acesso em 17 jan. 2023.

titular não atendida – após múltiplas tentativas – para que a companhia parasse de lhe enviar e-mails publicitários. Como a Rappi não possuía o consentimento prévio e expresso do titular para lhe direcionar *marketing* via e-mail, a SIC multou a empresa no valor de 500,3 milhões de pesos colombianos[350] e ainda definiu que os cidadãos do país não poderiam estar submetidos a nenhum tipo de ônus perante os controladores de dados – muito menos quando estes não tiverem recolhido o consentimento válido daqueles.[351] Este caso demonstra que, além de autoridades regulatórias da proteção de dados e do consumidor, as autoridades de defesa à concorrência podem também atuar concomitantemente às demais em benefício dos titulares de dados e consumidores, compondo a rede multissetorial regulatória a fim de salvaguardar os direitos dos cidadãos.

5. Por fim, a última sanção administrativa que vale ser destacada, inclusive pela sua relevância histórica, foi a multa de 6,6 milhões de reais, aplicada em 2019 e reestabelecida em 2022,[352] pela Senacon às empresas Facebook Inc. e Facebook Serviços Online do Brasil Ltda. – atualmente integrantes do grupo Meta – pelo compartilhamento indevido de dados pessoais de cerca de 443 mil usuários brasileiros que foram alvos da Cambridge Analytica.[353] À época dos fatos, a LGPD ainda não se encontrava em vigor no Brasil, porém a discussão sobre violação de consentimento, compartilhamento automático de dados e determinação de finalidades legais não foi impedida, tendo sido realizada à luz do CDC. A Senacon, além de constatar violações das empresas referentes ao seu dever de informação enquanto fornecedoras de serviços, averiguou uma má gestão dos dados pessoais sob seu tratamento, visto ter sido utilizado o modelo *opt-out* para a autorização de compartilhamento dos dados de terceiros. Esta conclusão da Senacon revela que práticas manipulatórias contra consumidores-titulares no ambiente digitalizado já ocorriam muito antes do protagonismo da LGPD para a resolução de conflitos na seara da proteção de dados, devendo ser dada prioridade por

[350] *Cf.: Rappi multada por violar protección de datos personales*, El Tiempo, 03 nov. 2021. Disponível em: <https://www.eltiempo.com/economia/empresas/rappi-multada-por-violar-proteccion-de-datos-personales-628739>. Acesso em 17 jan. 2023.
[351] *Idem.*
[352] *Cf.: Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários,* Ministério da Justiça e Segurança Pública, 23 ago. 2022. Disponível em: < https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios>. Acesso em 17 jan. 2023.
[353] *Cf.*: *MJSP multa Facebook em R$ 6,6 milhões,* Ministério da Justiça e Segurança Pública, 30 dez. 2019. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-multa-facebook-em-r-6-6-milhoes>. Acesso em 17 jan. 2023.

parte das autoridades regulatórias à defesa dos direitos e garantias dos titulares, principalmente daqueles relativos ao seu poder decisório.

Diante dos exemplos apresentados, cabe pontuar ainda que, se porventura for possibilitada a constatação, mediante procedimento administrativo, de práticas manipulatórias contra titulares de dados, ao avaliar **alto risco de gravidade, má-fé da empresa infratora e inexistência de mecanismos de mitigação de danos**,[354] a Autoridade Nacional de Proteção de Dados poderia – a partir da análise do caso concreto – aplicar imediatamente as sanções mais graves estipuladas nos incisos de V a XII do artigo 52 da LGPD. Essa seria uma medida alternativa ao *enforcement* por sanções gradativas prevista na lei de proteção de dados, visto a gravidade das consequências que a manipulação comportamental pode ter em face dos titulares.

Do mesmo modo, a Senacon pode cumulativamente aplicar sanções que considerar pertinentes com a gravidade da infração do caso concreto, sendo também relevantes para sua avaliação a **vantagem indevida auferida e a condição econômica do fornecedor**.[355] Considerando que, como relatado no capítulo 2 deste trabalho, o investimento e lucro de companhias vigilantes constituem um retorno econômico sem precedentes em *feedback looping* positivo para essas empresas, porém gerador de externalidades em *feedback looping* negativo para os consumidores-titulares, há de se concluir que a atuação de *enforcement* da Senacon pode ser mais severa quando os direitos dos consumidores forem claramente violados.

No que concerne às **medidas regulatórias *ex ante***, cabe destacar que a Autoridade Nacional de Proteção de Dados tem um papel central na elaboração de guias e manuais orientativos para os agentes econômicos privados, de maneira a direcioná-los tanto em relação às boas práticas que devem ser adotadas enquanto controladores e terceiros dentro do fluxo informacional,[356] quanto no que tange à vedação de práticas manipulatórias para a extração de dados pessoais de titulares. Ademais, à semelhança do que fez no *Guia Orientativo Cookies e proteção de Dados Pessoais*[357], a ANPD deve parametrizar, em suas publicações, quais devem

[354] Vide: Art. 52, §1º, I, II e VIII, da LGPD.
[355] Vide: Art. 57, do CDC.
[356] Vale pontuar que a ANPD já possui um Guia Orientativo que pormenoriza as definições de agentes de tratamento e do encarregado. – *Cf.*: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado*, Brasília, v. 2.0, abril de 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf>. Acesso em 15 jan. 2023.
[357] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo Cookies e proteção de Dados Pessoais*, Brasília, outubro de 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em 15 jan. 2023.

ser os princípios, hipóteses legais e conceitos imprescindíveis para o desenvolvimento de determinadas atividades econômicas envolvendo o tratamento de dados pessoais – sendo estes sensíveis ou não – por agentes econômicos de grande relevância no mercado, a exemplo de plataformas digitais e *big techs*.

O que se observa até o momento, pela análise de guias, notas técnicas, resoluções e relatórios até agora publicados,[358] é que a Autoridade, nestes primeiros anos de atuação, tem priorizado a orientação e a condução de atores públicos e de agentes privados de pequeno porte – deixando de lado as grandes empresas de tecnologia por ora. Tal situação decorre de demandas desses atores[359] que, indubitavelmente, a ANPD tem de atender enquanto autarquia federal atuante em prol da defesa dos direitos dos titulares de dados. Todavia, propõe-se, neste momento, uma maior atenção por parte da Autoridade às entidades privadas vigilantes responsáveis pelo emprego de técnicas manipulativas para a extração de dados pessoais de titulares.

Isso porque, a partir de uma regulação *ex ante*, através da adoção de uma postura preventiva consubstanciada por documentos oficiais, a ANPD pode, ao menos em certa medida, mitigar os riscos que tais agentes trazem, ao proporem-se a utilizar métodos persuasivos de manipulação, aos titulares de dados. Ao estabelecer explicitamente vedações a tais práticas manipulativas por publicações oficiais, a Autoridade regula, de maneira precaucional, atores econômicos de grande significância e impacto sobre os titulares de dados; e, assim, otimiza a tutela jurídica de seus direitos e salvaguardas.

Um exemplo seria a criação pela ANPD de um **guia orientativo destinado aos próprios titulares de dados**, a fim de que possam se resguardar em relação às ***dark patterns*** mais utilizadas por *websites*, aplicativos e mídias sociais. O documento poderia conter, em linguagem acessível ao titular: i) o conceito de *dark pattern*; ii) tipologias mais comuns de padrões obscuros; iii) quais os impactos de cada tipologia nos direitos e salvaguardas do titular; iv) medidas que o titular poderia adotar para identificar os padrões existentes e dirimir o viés manipulatório empregado pelos agentes que se utilizam de tais técnicas.

---

[358] *Cf.*: *Publicações da ANPD*. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em 15 jan. 2023.

[359] Em conversa com a Diretora da ANPD, Miriam Wimmer, em reunião do grupo de pesquisa da USP *Núcleo de Direito Concorrencial e Economia Digital* (NUCED), no dia 08 de junho de 2022, a Diretora elucidou-me que a Autoridade, ao menos até aquele momento, estava ainda em estágios muito iniciais de atuação. Por esse motivo, não havia incluído em sua agenda de atuação a questões relativas à manipulação comportamental de titulares de dados, economia da atenção e *hipernudges*.

Outra medida interessante seria a publicação de recomendação ou guia referente a **diretrizes técnicas e éticas** que devem ser observadas em **pesquisas de *neuromarketing***, visando a garantia de direitos dos titulares submetidos a tais experimentos. Por exemplo, a Autoridade poderia definir: i) os princípios da LGPD e da Constituição Federal que as empresas devem se pautar para realizarem as pesquisas; ii) a base legal do consentimento enquanto hipótese necessária para o tratamento de dados pessoais por entidades privadas que almejem executar tais pesquisas; iii) os limites em relação às finalidades que pretendem ser alcançadas – se são para manipulação posterior do consumidor-titular, a ANPD há de considerá-las como ilícitas.

Por fim, vale pontuar que uma lacuna a ser preenchida pela ANPD relativa à **conduta de** agentes vigilantes, a fim de se evitar a manipulação comportamental de titulares, refere-se aos **birôs de crédito**. Torna-se de suma relevância a elaboração de documentação orientativa explanando quais são: i) seus limites de atuação, segundo a Lei do Cadastro Positivo e a LGPD; ii) os princípios que devem reger suas atividades de tratamento, com ênfase nos da necessidade e da não discriminação; iii) seus deveres enquanto controladores ou terceiros na cadeia de tratamento; e iv) as medidas de mitigação a serem adotadas em prol dos titulares de dados.

Portanto, Autoridade Nacional de Proteção de Dados e Secretaria Nacional do Consumidor, em conjunto com outras autoridades que compõem a estrutura regulatória multissetorial brasileira, devem atuar convergentemente para, ao avaliarem casos de manipulação comportamental por entidades privadas contra consumidores-titulares, aplicarem as medidas de *accountability* e *enforcement* – *ex post* e *ex ante* – cabíveis a cada situação concreta. Em decorrência da gravidade de certos casos a direitos dos titulares, é possível que ambos os atores intervenham de maneira preventiva ou reativa mais severa, a fim de assegurar a autodeterminação e o livre arbítrio do cidadão frente às ameaças de cunho manipulativo.

Cabe, finalmente, mencionar alguns mecanismos práticos de empoderamento dos titulares para que estes possam se engajar no monitoramento de quem os monitora constantemente – independentemente ou não das medidas regulatórias acima mencionadas –, a fim de possibilitar-lhes o uso de ferramentas para uma tomada de decisão mais livre de vícios, erros e persuasões.

6.2 – Ferramentas de contravigilância: como obter transparência em um mundo digital opaco

As primeiras ferramentas[360] que proporemos neste subcapítulo tratam-se de medidas disponíveis online para que o titular obtenha maior transparência por parte do algoritmo de uma *big tech* específica: o Facebook (grupo Meta).[361] Todas expõem como essa *big tech* perfiliza os seus usuários para posterior *marketing* direcionado com alto nível de precisão algorítmica e uma delas abrange a averiguação de transparência de outras empresas de tecnologia para fins de combate à desinformação. Vejamos a seguir quais são elas.

1. **What Facebook Thinks You Like**: é uma extensão do Google Chrome arquitetada pela instituição sem fins lucrativos ProPublica que coleta dados pessoais dos titulares, sob garantia de sua proteção e anonimização, para simular o processo de algoritmização do Facebook. A partir das informações inferidas, a ferramenta é capaz de retornar ao titular conteúdos relacionados às mais de 1.300 categorias de segmentação de anúncios[362] disponíveis para targetização publicitária às quais pode estar submetido, dependendo dos dados que fornece à *big tech* – seja por meio de *likes*, postagens, comentários ou visualizações.

2. **Data Selfie**: também uma extensão do Google Chrome, que analisa os traços digitais do titular deixados no Facebook, emitindo um relatório detalhado sobre o potencial de agregação e análise dos dados que o uso diário pelo usuário proporciona. Através do emprego de *machine learning*, o Data Selfie reúne tópicos como "Preferências" e "Keyword" para reunir quais dados são tratados pela big tech relacionados a gostos e sentimentos do usuário a partir das palavras-chave mais utilizadas no seu *feed*.[363]

3. **ProPublica Political Ad Collector**: em uma tradução literal, este "coletor de propagandas políticas", disponível para instalação no Chrome e no Firefox, permite

[360] A metodologia deste subcapítulo é baseada em artigo conduzido pelo Coding Rights, com complementos especificados pontualmente. *Cf.*: VARON, Joana; TEIXEIRA, Lucas. *Podemos vigiar os vigilantes?* Coding Rights, 2018, Boletim Antiviligância nº 16, 2018. Disponível em: <https://medium.com/codingrights/podemos-vigiar-os-vigilantes-ac3fe77e7694>. Acesso em 22 dez. 2022.

[361] O grupo Meta é constituído por Facebook e Instagram, cuja utilização pelos titulares de dados brasileiros, em um total de cerca de 159 milhões de usuários, é de 85%, 86% e 84% respectivamente. – *Cf.*: <https://www.nic.br/noticia/na-midia/87-dos-brasileiros-serao-usuarios-de-redes-sociais-em-2026/>. Acesso em: 22 dez. 2022.

[362] *Cf.*: ANGWIN, Julia; PARRIS JR., Terry; MATTU; Surya. *Breaking The Black Box*: What Facebook Knows About You, ProPublica, 2016. Disponível em: <https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you>. Acesso em 22 dez. 2022.

[363] *Cf.*: *Data Selfie segue todos os seus passos no Facebook*. Disponível em: <https://www.techtudo.com.br/tudo-sobre/data-selfie/>. Acesso em: 22 dez. 2022.

compartilhar com a ProPublica – de maneira desvinculada com a identidade do titular – as publicidades que são divulgadas em seu *feed* do Facebook. Por meio de uma separação de quais dessas publicidades são propagandas políticas, o resultado é utilizado para estudos da própria instituição sem fins lucrativos e para conferir transparência aos usuários da *big tech* sobre como o algoritmo utiliza seus dados ao segmentar as propagandas políticas a partir da sua geolocalização, idade e posicionamento político inferido.[364]

4. **Who Targets Me**: também uma extensão do Chrome e do Firefox, confere ao titular a possibilidade de constatar "de quem é alvo" no mundo *online* em relação às publicidades direcionadas, com destaque às targetizações políticas ocorridas no Facebook. A ferramenta permite a criação de perfis anônimos que coletam dados pessoais e os relacionam a propagandas políticas – bem como a outras modalidades de *microtargeting* – para justificar ao titular, de acordo com o algoritmo da *big tech* ou plataforma específica, por que lhes foram direcionados tais anúncios publicitários. O Who Targets Me ainda fornece estatísticas sobre quais empresas têm "mirado" mais o titular e construído banco de dados de publicidade e direcionamento político com suas informações pessoais.[365]

As últimas ferramentas propostas constituem outras modalidades de engajamento dos titulares, relativas à promoção de melhor entendimento do usuário de aplicativos e plataformas digitais sobre os algoritmos que processam seus dados, bem como à detecção de perfis falsos *online* e medidas que incrementem a proteção de seus dados pessoais. Confiramos abaixo.

5. **Facebook Tracking Exposed**: esta extensão do Firefox e do Chrome possibilita o repasse de informações ao titular sobre os posts que aparecem em seu *feed* do Facebook.[366] O titular não necessita revelar seus dados pessoais, pois apenas são avaliados *posts* públicos para inferir, observar e avaliar o algoritmo da plataforma, em especial como esta operacionaliza quais posts aparecem ao usuário – bem como a sua ordem. As informações obtidas dos *posts* públicos são agregadas em uma base de dados do Facebook Tracking Exposed para informar ao titular quais conteúdos direcionam ou disputam mais sua atenção enquanto navega pelo *feed*.

---

[364] *Cf.*: *Facebook Political Ad Collector*: How Political Advertisers Target You. Disponível em: <https://projects.propublica.org/facebook-ads/>. Acesso em: 22 dez. 2022.
[365] *Cf.*: *Who Targets Me*. Disponível em: <https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/who-targets-me.html>. Acesso em: 22 dez. 2022.
[366] *Cf.*: *Make an accessible framework so anyone can analyze Facebook's newsfeed algorithm.* Disponível em: <https://facebook.tracking.exposed/>. Acesso em 22 dez. 2022.

6. **Eleições Sem Fake**: trata-se de um projeto desenvolvido pela Universidade Federal de Minas Gerais (UFMG), que visa à detecção de perfis fakes (*bots*) em redes sociais, com fins de combate à desinformação nas eleições. O site do projeto abrange *plug-ins* para WhatsApp, Telegram e Facebook para que o titular possa fazer a constatação de targetização falsa desde publicidade direcionada até verificação de hashtags mais utilizadas promovidas por *bots* – bem como promove ferramentas de verificação de *fake news*.[367]

7. **Privacy Badger**: é uma extensão disponível para Chrome, Firefox e Opera que busca impedir a vigilância online realizada por *trackers* de navegação online. Os trackers se utilizam dos rastros digitais que o titular deixa *online* ao visitar páginas de sites e aplicativos de plataformas digitais através do carregamento de *scripts*. O Privacy Badger não bloqueia todos os *scripts* – inutilizando os sites e plataformas –, e sim se utiliza de inteligência artificial para separar *scripts* de monitoramento de histórico de navegação do titular daqueles estritamente necessário para as plenas funcionalidades dos sites e plataformas.[368]

8. **Mozilla Container**: é uma ferramenta vinculada ao Facebook e, como o próprio nome sugere, a extensão é passível de instalação apenas para o Firefox. O Mozilla Container omite a identidade do titular registrada no Facebook, impedindo que os *scripts* da *big tech* acessem seus dados pessoais de outras bases abertas no navegador por meio de *cookies* de terceiros (*third-party cookies*).

Todas as ferramentas sugeridas neste subcapítulo constituem medidas de contravigilância capazes de serem usadas por parte dos cidadãos contra quem os monitora constantemente, usualmente utilizando-se de técnicas manipulatórias que tolhem os titulares de dados de sua capacidade de discernimento quanto ao tratamento de seus dados pessoais. Por meio de seu emprego, os titulares de dados possuem maiores probabilidades de defesa contra a vigília massiva e a manipulação de plataformas digitais e *big techs*, principalmente no que tange às práticas de *marketing* direcionado, à desinformação e ao modelo do gancho (vide subcapítulo 3.2).

[367] *Cf.*: *Projeto Eleições Sem Fake*. Disponível em: <https://www.eleicoes-sem-fake.dcc.ufmg.br/>. Acesso em 22 dez. 2022.
[368] *Cf.*: *Privacy Badger is a browser extension that automatically learns to block invisible trackers*. Disponível em: <https://privacybadger.org/>. Acesso em: 22 dez. 2022.

Em conclusão, a importância das propostas trazidas neste capítulo 6 se baseia na necessidade de se assegurar a simetria informacional e manifestação da vontade livre, inequívoca e informada dos cidadãos-titulares em uma ordem econômica datificada, cujo ordenamento jurídico tutela os direitos à proteção de dados pessoais e à autodeterminação informativa sob um prisma humanista**.** Os intérpretes do direito, bem como os atores regulatórios, hão de visualizar os consumidores-titulares sob as lentes de suas potencialidades deliberativas para que, assim, **exista liberdade decisória em meio a um panóptico manipulatório orquestrado à modulação de (con)sentimentos**.

CONCLUSÃO

Pudemos constatar, neste trabalho, que o amálgama entre seres humanos e o mundo digitalizado é inevitável. Os riscos apresentados pelo capitalismo de vigilância datificado – apontados no capítulo 1 – transpassam as barreiras palpáveis e se transvestem de benefícios em troca de funcionalidades práticas a fim de extraírem o máximo de tempo, atenção e dados dos titulares. Isso porque toda a noção de positividade do psicopoder que orienta a sociedade contemporânea abre margem para que entidades privadas possam manipular comportamentos e, por conseguinte, (con)sentimentos e processos cognitivos.

A identificação dessas entidades – no capítulo 2 – enquanto não apenas plataformas digitais e *big techs*, mas também empresas varejistas, companhias aéreas, birôs de crédito, dentre outros atores de variados setores econômicos; bem como a averiguação das práticas manipulativas – no capítulo 3 – proporcionaram o entendimento de como se dá a violação massiva dos sentimentos e da cognição dos indivíduos na economia digital. Através da sua submissão a **i)** *(hiper)nudges*, **ii)** *dark patterns*, **iii)** processos de dissonância cognitiva, **iv)** modelos de captura e engajamento da atenção, **v)** psicometria analítica, **vi)** matematização de expressões faciais e **vii)** pesquisas intrusivas de *neuromaketing*, os atores vigilantes se apresentam enquanto ameaças não apenas de cunho psicológico, mas também aos direitos e salvaguardas dos cidadãos inseridos no panóptico manipulatório orquestrado à modulação comportamental.

Tais constatações justificaram a necessidade de se compreender o arcabouço jurídico conferido pela legislação brasileira relativo à proteção de dados pessoais e ao consentimento dos titulares-consumidores, em breves comparações às Guidelines de nº 5 do European Data Protection Board – no capítulo 4. A partir da compreensão dos princípios norteadores e requisitos de tratamento de dados pessoais, foi possível concluir que a base legal do consentimento, apesar de não ser hierarquicamente superior às demais estipuladas pela Lei Geral de Proteção de Dados, possuía primazia neste trabalho e deveria ser adotada – de acordo com os parâmetros e adjetivações preconizados pela LGPD – para configurar a licitude do tratamento de dados pelas entidades privadas configuradas como controladoras e fornecedoras de produtos e serviços neste trabalho.

Ademais, o estudo das violações jurídicas específicas – no capítulo 5 – conferiu-nos a possibilidade de comparar a óptica behaviorista dos atores vigilantes com a visão humanista do

ordenamento jurídico favorável à liberdade volitiva do cidadão: enquanto os primeiros o coloca em uma posição de cobaias experimentais de fácil manipulação; o segundo, ainda que considere a vulnerabilidade do titular como corolário da falácia de sua soberania, o faz por ponderar a necessidade de garantir-lhe a autodeterminação em seus processos decisórios. Tal constatação repercutiu na proposta – no capítulo 6 – de medidas de *accountability* e *enforcement* – *ex post* e *ex ante* – por parte da Autoridade Nacional de Proteção de Dados e da Secretaria Nacional do Consumidor enquanto atores regulatórios essenciais em uma governança multissetorial em benefício dos consumidores-titulares*;* assim como de mecanismos de contravigilância capazes de reforçar o consentimento livre, inequívoco e informado dos cidadãos.

A partir disso, este trabalho de conclusão de curso é encerrado enfatizando-se a importância de nos desvincularmos, mesmo que pouco a pouco, deste processo retroalimentar de vigília incógnita fomentado tanto pela manipulação "extraorientativa", quanto pela autoexploração em busca do êxito superprodutivo. Assim, finaliza-se por meio de uma metafórica inserção de reticências em um inevitável ponto final, mediante uma citação do psicólogo Carl Rogers, no anseio de que a tomada de decisão sob o prisma humanista possa transcender os fundamentos jurídicos e encontrar materialidade no mundo digitalizado.

"Quando essa capacidade única de ser consciente que o homem possui funciona dessa forma livre e integral, vemos que temos diante de nós, [...] não uma besta que devemos controlar, mas um organismo capaz de alcançar, graças à notável capacidade integrativa do seu sistema nervoso central, um comportamento equilibrado, realista, valorizando-se a si mesmo e valorizando o outro, comportamento que é a resultante de todos esses elementos da consciência."

CARL ROGERS[369]

[369] ROGERS, Carl. *Tornar-se pessoa*, São Paulo: WMF Martins Fontes, 2017, p. 115.

REFERÊNCIAS BIBLIOGRÁFICAS

ANGWIN, Julia; PARRIS JR., Terry; MATTU; Surya. *Breaking The Black Box*: What Facebook Knows About You, ProPublica, 2016. Disponível em: <https://www.propublica.org/article/breaking-the-black-box-what-facebook-knows-about-you>. Acesso em 22 dez. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia Orientativo*: Cookies e proteção de dados pessoais, publicado em outubro de 2022. Brasília, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em 20 nov. 2022.

ÁVILA, Flávia; BIANCHI, Ana Maria. (org.). *Guia de Economia Comportamental e Experimental*, 2ª ed., São Paulo: InBehavior Lab, pp. 26-60, 2019.

BACHRACH, Yoram et al. Personality and patterns of Facebook usage. *In: Proceedings of the 4th annual ACM web science conference*, 2012.

BARBOSA, Fernanda Nunes. Informação: direito e dever nas relações de consumo. São Paulo: Revista dos Tribunais, 2008.

BARBOSA, Katiuscia de Azevedo et al. *A técnica de condicionamento operante dentro do laboratório*, João Pessoa: X Encontro de Iniciação à Docência, UFPB-PRG, 2007.

BARRETT, Lisa Feldman et al. *Emotional expressions reconsidered:* Challenges to inferring emotion from human facial movements. Psychological science in the public interest, v. 20, n. 1, 2019.

BENTES, Anna. *A gestão algorítmica*: enganchar, conhecer e persuadir. Políticas, Internet e Sociedade, Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2019.

BENTES, Anna. *Quase um tique*: economia da atenção, vigilância e espetáculo em uma rede social, Rio de Janeiro: Ed. UFRJ, 2021.

BERCEA, Monica D. *Anatomy of methodologies for measuring consumer behavior in neuromarketing research*, 2012.

BIONI, Bruno Ricardo. Legítimo interesse: aspectos gerais a partir de uma visão obrigacional. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023.

_____; KITAYAMA, Marina; RIELLI, Mariana. *O Legítimo Interesse na LGPD:* quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021, p. 23. Disponível em: <https://www.observatorioprivacidade.com.br/2021/01/29/legitimo-interesse-na-lgpd-quadro-geral-e-exemplos-de-aplicacao/>. Acesso em 05 dez. 2022.

_____. *Proteção de dados:* a função e os limites do consentimento, 3ª ed., Rio de Janeiro: Forense, 2021.

_____. *Regulação e proteção de dados pessoais*: o princípio da accountability, 1ª Ed.,Rio de Janeiro: Forense, 2022.

BRASIL. *Constituição da República Federativa do Brasil de 1988*, Brasília, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 04 dez. 2022.

_____. Lei nº 13.709, de 14 ago. 2018, *Lei Geral de Proteção de Dados Pessoais* (LGPD), Brasília, DF. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>, Acesso em 15 nov. 2022.

_____. *Lei nº 13.709, de 14 ago. 2018*, Lei Geral de Proteção de Dados Pessoais (LGPD), Brasília, 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 05 dez. 2022.

_____. Lei 12.414, de 09 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, Brasília, 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em 20 dez. 2022.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências, Brasília, 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 17 dez. 2022.

_____. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, Brasília, 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

_____. *Lei nº 12.527, de 18 de novembro de 2011*. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. 2011. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em 10 dez. 2022.

_____. Superior Tribunal de Justiça, REsp 1.419.697/RS, Rel. Min. Paulo de Tarso Sanseverino, Brasília. Data de Julgamento: 12/11/2014. Data de Publicação DJe: 17/11/2014. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=39037908&num_registro=201303862850&data=20141117&tipo=51&formato=PDF>. Acesso em: 17 dez. 2022.

BRUNO, Fernanda Glória. *A economia psíquica dos algoritmos:* quando o laboratório é o mundo. NEXO Jornal, Brasil, pp. 1-3, 12 jun. 2018.

BULL, Hans-Peter. *Informationelle Selbstbestimmung*: Vision oder Illusion?, Tübinger:Mohr Siebeck, 2009, p. 29.

CALIMAN, Luciana Vieira. *A biologia moral da atenção*: a constituição do sujeito (des)atento. Tese de Doutorado em Saúde Coletiva, Universidade do Estado do Rio de Janeiro, Instituto de Medicina Social, Rio de Janeiro, 2006.

CALO, Ryan. *Against notice skepticism in privacy (and elsewhere).* Notre Dame Law Review, v. 87, n. 3, 2011.

CARSTENS, Agustín et al. Regulating big techs in finance, BIS Bulletin, n. 45, 2021.

CASTELLS, Manuel. Communication, power and counter-power in the network society. *International journal of communication*, v.1, n.1, 2007.

CLARKE, Roger. Profiling: A hidden challenge to the regulation of data surveillance. *Journal of Law & Information Science*, v. 4, p. 403, 1993.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Cookies:* sanction de 60 millions d'euros à l'encontre de MICROSOFT IRELAND OPERATIONS LIMITED, 22 décembre 2022. Disponível em: <https://www.cnil.fr/fr/cookies-sanction-de-60-millions-deuros-lencontre-de-microsoft-ireland-operations-limited>. Acesso em 15 jan. 2023.

CONSELHO ADMINISTRATIVO DE DEFESA DA CONCORRÊNCIA. *Cartilha do CADE*, Atualização: maio de 2016. Disponível em: <https://cdn.cade.gov.br/Portal/acesso-a-informacao/perguntas-frequentes/cartilha-do-cade.pdf>. Acesso em 17 jan. 2023.

COSTA JR, Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: RT, 1995.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

_____. Panorama histórico da proteção de dados pessoais. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023.

DWORKIN, Ronald. *Levando os direitos a sério*, São Paulo: Martins Fontes, 2002.

E-SPIN. Types of Privacy Enhancing Technologies and their examples. *In: Global Themes and Features Topics, Industries, Information Technology*, publicado em 18. nov. 2021. Disponível em: <https://www.e-spincorp.com/types-of-privacy-enhancing-technologies-and-their-examples/>. Acesso em 15. dez. 2022.

EKMAN, Paul. Universals and Cultural Differences in Facial Expressions of Emotions. *In:* COLE, J. (Ed.), *Nebraska Symposium on Motivation*, v. 19, Lincoln, NB: University of Nebraska Press, 1972.

ENJOLRAS, Franck. *Gare à ces 'algorithmes qui pourraient finir par nous connaître mieux que nous nous connaissons nous-mêmes'*. Le Monde, publicado em 26 dez. 2018. Disponível em: <https://www.lemonde.fr/sciences/article/2017/12/26/gare-a-ces-algorithmes-qui-nous-connaissent-mieux-que-nous-memes_5234390_1650684.html#:~:text=Par%20leur%20analyse%2C%20des%20algorithmes,mettre%20fin%20%C3%A0%20nos%20jours.>. Acesso em: 15 jun. 2019.

ESTADOS UNIDOS. U.S Department of Health, Education and Welfare (HEW). *Records, Computers and the Rights of Citizens*: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Library Department of Justice, 1973. Disponível em: <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. Acesso em: 29 nov. 2022.

EVANS, Davis S.; SCHMALENSEE, Richard. *The Antitrust Analysis of Multi-Sided Platform Business*, Cambridge, NBER Working Paper n. 18783, 2013.

EYAL, Nir; HOOVER, Ryan. *Hooked:* How to Build Habit-Forming Products, Portfolio Penguin, 2014.

FESTINGER, Leon A. *A theory of cognitive dissonance*, Evanston, II: Row. Peterson, 1957.

FOUCAULT, Michel. *A vontade de saber*: Sexualidade e verdade I. Frankfurt a. M., 1977.

_____. *Vigiar e punir*: nascimento da prisão, 27ª ed., Petrópolis: Vozes, 1999.

FOGG, Brian J. *A Behavior Model for Persuasive Design*, Persuasive Technology Lab Stanford University, 2009.

FRANKL, Viktor. *Em Busca de Sentido:* um psicólogo no campo de concentração. 39ª ed., Petrópolis: Vozes, 2016.

FRAZÃO, Ana. *A falácia da soberania do consumidor*. O aumento da vulnerabilidade do consumidor na economia digital. Publicado em: 08/12/2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-emercado/falacia-soberania-do-consumidor-08122021>. Acesso em 20 nov. 2022.

_____; TEPEDINO, Gustavo; OLIVA, Milena Donato. *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*, São Paulo: Revista dos Tribunais, Thomson Reuters, 2019.

_____. Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência. In: *Empresa, Mercado e Tecnologia*, 2019.

_____. Big Data, Plataformas Digitais e Principais impactos sobre o direito da concorrência. In: *Empresa, Mercado e Tecnologia*, 2019.

_____. *Economia como um sistema de crenças*. Entendendo os bastidores do debate econômico a partir da obra de John Kenneth Galbraith, Jota, publicado em 14 dez. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/economia-como-um-sistema-de-crencas-14122022>. Acesso em 08 jan. 2023.

_____; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Editora Revista dos Tribunais, 2019.

_____. *'Neurocapitalismo' e o negócio de dados cerebrais:* Os nossos pensamentos e a nossa identidade pessoal estão em risco? Publicado em: 25 set. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/neurocapitalismo-e-o-negocio-de-dados-cerebrais-25092019>. Acesso em 24 nov. 2022.

_____. *Nova LGPD*: o tratamento dos dados pessoais sensíveis. Jota, publicado em 26 set. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018>. Acesso em 16 dez. 2022.

_____. *O mito da soberania do consumidor*. É legítimo esperar que as soluções de mercado protejam o consumidor?, Jota, publicado em 01 dez. 2021. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-mito-da-soberania-do-consumidor-01122021>. Acesso em: 08 jan. 2023.

_____. Proteção de dados pessoais e democracia: a ameaça da manipulação informacional e digital. In: *A Lei Geral de Proteção de Dados LGPD*. Revista dos Tribunais, 2021.

FREUD, Sigmund. Cinco lições de psicanálise, In: *Obras Psicológicas Completas de Sigmund Freud*, XI. Imago, 1910.

GOLDBERG, Lewis R. *The structure of phenotypic personality traits*. American psychologist, v. 48(1), n. 26, 1993.

GOLDBECK, Jennifer; MAURIELLO, Matthew. *User perception of Facebook app data access: a comparison of methods and privacy concerns*. Future Internet, v. 8, n. 2, 106.

GRAY, Colin M.; et. al. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI'18. ACM, New York, NY, USA, Article 534, 2018.

GUILHARDI, Hélio J. *Auto-estima, autoconfiança e responsabilidad*e, Instituo TCR, Orgs.: Maria Zilah da Silva Brandão, Fatima Cristina de Souza Conte, Solange Maria B. Mezzaroba. Santo André, SP: ESETec Editores Associados, 2002.

HAGLU, Andrei; WRIGHT, Julian. Multi-Sided Platforms, *International Journal of Industrial Organization*, vol. 43, issue C, 2015.

HAN, Byung-Chul. *No exame*: perspectivas do digital, Petrópolis, RJ: Vozes, 2018.

_____l. *Sociedade do Cansaço*, 2ª ed. ampliada, Petrópolis, RJ: Vozes, 2017.

HARARI, Yuval Noah. *21 lições para o século 21*. São Paulo: Companhia das Letras. Edição do Kindle.

HASHEM, Ibrahim et al. The rise of "big data" on cloud computing: review and open research issues. *Information systems*. v. 47, pp. 98-115, 2015.

HOFFMANN-RIEM, Wolfgang. *Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información*, ReDCE, n. 22, 2014.

JACÓ-VILELA, Ana Maria; FERREIRA, Arthur Arruda Leal; PORTUGAL, Francisco. *História da psicologia*: rumos e percursos, Rio de Janeiro: Nau Editora, 2006.

JAYME, Erik. Identité culturelle et intégration: le droit internationale privé postmoderne. In: JAYME, Erik. *Recueil des Cours de l'Ácadémie de Droit International de La Haye*. Doordrecht: Kluwer, 1995.

KAHNEMAN, Daniel. *Rápido e Devagar.* Duas formas de pensar. Tradução de Cassio Leite, São Paulo: Objetiva, 2011.

KANASHIRO, Marta M. Apresentação*: Vigiar e resistir*: a constituição de praticas e saberes em torno da informação. Ciência e Cultura, v. 68, n. 1, p. 20-24, 2016. DOS REIS PERON, Alcides Eduardo; ALVAREZ, Marcos César; CAMPELLO, Ricardo Urquizas. Apresentação do Dossiê: *Vigilância, Controle e Novas tecnologias*. Mediações-Revista de Ciências Sociais, v. 23, n. 1, 2017.

KATZ, Michael; SHAPIRO, Carl. Network externalities, competition and compatibility. The American economic review, v. 75, n. 3, pp. 424-440, 1985.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. Editora Revista dos Tribunais, 2019.

KOSINSKI, Michal; STILLWELL, David; GRAEPEL, Thore. *Private traits and attributes are predictable from digital records of human behavior,* PNAS, Washington, DC, v. 110, n. 15, pp. 5802-5805, 2013.

KUHN, Thomas S. *A estrutura das revoluções científicas*, 5ª edição, São Paulo: Editora Perspectiva, 1998.

LAW, Thomas. *A Lei Geral de Proteção de Dados:* uma análise comparada ao novo modelo chinês, 1ª ed., Belo Horizonte, São Paulo: D'Plácido, 2021.

LESSIG, Lawrence. *Reading The Constitution in Cyberspace*. Emory Law Review, v. 45, 1996.

LIMA, Caio César C. Seção I – Dos requisitos para o tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato (coord.). *LGPD – Lei Geral de Proteção de Dados*. São Paulo: RT, 2019, p. 184.

LUGURI, Jamie; STRAHILEVITZ, Jacob. Shining a light on dark patterns, *Oxford University Press*, The John M. Olin Center for Law, Economics and Business at Harvard Law School, 2021.

MARCIANO, Alain et al. Big data and big techs: understanding the value of information in platform capitalism, *European Journal of Law and Economics*, Springer, n. 50, pp. 345–358, 2020.

MARQUES, Claudia Lima; BENJAMIN, Antônio Herman; MIRAGEM, Bruno. *Comentários ao Código de Defesa do Consumidor*. 3ª ed. São Paulo: RT, 2010.

_____; MIRAGEM, Bruno. O necessário diálogo entre a LGPD e o Código de Defesa do Consumidor e os novos direitos do consumidor-titular dos dados. In: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023.

MARTINS, Leonardo. (org.) *Cinquenta anos de Jurisprudência do Tribunal Constitucional federal Alemão*. Montevidéu: Fundação Konrad Adenauer, 2005.

MENDES, Laura Schertel. *Habeas data e autodeterminação informativa*: dois lados da mesma moeda, Direitos Fundamentais & Justiça, Belo Horizonte, v. 12, n. 39.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*, v. 120, pp. 469-493, nov.-dez., 2018.

_____ et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023, p. 22.

MENEZES CORDEIRO, Antonio Manuel da Rocha e. *Da boa-fé no Direito Civil*, Coimbra: Almedina, 2011.

NADLER, J.; CICILLINE, D. N. Investigation of Competition in Digital Markets, Majority Staff Report and Recommendations, *Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary*, 2020.

NEUTZLING FRAGA, P. *Atitude do Consumidor: o Caminho para a Persuasão*, VIII Congresso Brasileiro de Ciências da Comunicação da Região Sul, Passo Fundo, RS: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, 2007.

NEVES, João Marcos Santos das. *Proteção de dados na internet a partir do estudo de caso Cambridge Analytica*: parâmetros para um debate internacional, Trabalho de Conclusão de Curso, Universidade Federal Fluminense, Macaé, 2020.

O'NEIL, Cathy. *Weapons of math destruction*: How big data increases inequality and threatens democracy. Broadway Books, 2016.

OCDE. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. OECD Publishing, Paris, 2019, p. 20-23. Disponível em: <https://read.oecd-ilibrary.org/science-and-technology/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation_53e5f593-en#page22>. Acesso em: 15 de nov. 2022.

PASQUALE, Frank. *The black box society*. The secret algorithms that control money and information, Cambridge: Harvard University Press, 2015.

RIVEROS AEDO, Edgardo. *La psicología humanista: sus orígenes y su significado en el mundo de la psicoterapia a medio siglo de existência*. Ajayu, Órgano de Difusión Científica del Departamento de Psicología de la Universidad Católica Boliviana San Pablo, v. 12, n. 2, pp. 135- 186, 2014.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROGERS, Carl. *Tornar-se pessoa*, São Paulo: WMF Martins Fontes, 2017.

SANTOS, Isabela de Araújo. *A vulnerabilidade dos titulares de dados diante de grandes plataformas digitais e big techs*: um paralelo entre as violações ao GDPR e à LGPD no que tange à base legal do consentimento. Brasília: Revista dos Estudantes de Direito da Universidade de Brasília, 2022.

_____; ARAÚJO, Tayná Frota de. Liberdade, previsão, ação: desafios da Lei de Liberdade Econômica sob o viés da Economia Comportamental. In: FRAZÃO, Ana; PRATA DE CARVLHO, Angelo. *Lei de Liberdade Econômica*: análise crítica, 1ª ed., Rio de Janeiro: Forense, 2022.

_____. *Manipulação comportamental em uma economia datificada:* uma análise de métodos de persuasão da psicologia para obtenção de dados no capitalismo de vigilância, publicado em 03 mar. 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/comportamento-manipulacao-comportamental-na-economia-datificada-03032022>. Acesso em 21 nov. 2022.

SILVEIRA, Heitor Vicente da et al. Usos do termo emoção na obra de B. F. Skinner. Acta Comportamentalia, *Revista Latina de Análise de Comportamiento*, v. 27, n. 4, 2019.

SIMON, Herbert. Designing organizations for an information-rich world. In: GREENBERGER, M. *Computers, communications and the public interest*. Baltimore: The John Hopkins Press, 1917.

SKINNER, Burrhus F. O lugar do sentimento na análise do comportamento. *In*: *Questões recentes na análise comportamental*. Campinas, SP: Papirus. Cap. 1, 1991.

_____. *Para além da liberdade e da dignidade*. Lisboa: Edições 70, 2000.

SOUZA, Cid Marconi Gurgel de; CARRÁ, Bruno Leonardo Câmara. A hierarquia das necessidades de Maslow e os danos extrapatrimoniais: um paralelo entre o Direito e a Psicologia Humanista. *Revista de Informação Legislativa*: RIL, Brasília, DF, v. 59, n. 234, pp. 11-33, 2022

SOUZA, Luciana Cristina et al. *Análise crítica da orientação de cidadãos como método para otimizar decisões públicas por meio da técnica nudge*, *In*: Revista Brasileira de Políticas Públicas - Programa de Mestrado e Doutorado em Direito do UniCEUB. Vol. 8, n. 2 (ago. 2018). Brasília: UniCEUB, 2011.

SUNDMAEKER, Harald et al. Vision and challenges for realizing the Internet of Things. *Cluster of European Research Projects in the Internet of Things*, European Commission, v. 3, n. 3, 2010.

SUNSTEIN, Cass R.; THALER, Richard H. *Nudge:* Improving Decisions About Health, Wealth, and Happiness. New Haven: Yale University Press, 2008.

_____. *A verdade sobre os boatos*: como se espalham e por que acreditamos neles. Rio de Janeiro: Elsevier, 2010.

TEIXEIRA, Tarcísio (coord.). *Proteção de dados*, São Paulo: Editora Jvspodium, 2020.

THE ECONOMIST. *The new titans.* And how to tame them. 20 jan. 2018. Disponível em: <https://www.economist.com/leaders/2018/01/18/how-to-tame-the-tech-titans>. Acesso em: 15 nov. 2022.

TURNER, Ash. *Smartphone addiction facts & phone usage statistics the definitive guide* (2020-2021 Update) Disponível em: <https://www.bankmycell.com/blog/smartphone-addiction/#chap-ter0>. Acesso em 23 nov. 2022.

UNIÃO EUROPEIA. *Guidelines 05/2020 on consent under Regulation 2016/679*, Adopted on 4 May 2020, p. 10. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pt>, Acesso em: 7 dez. 2022.

_____. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, Art. 4 (11)**:** Definitions, 2016. Disponível em: <https://gdpr-info.eu/art-4-gdpr/>, Acesso em: 07 dez. 2022.

VAN DE VEN, Ruben. *Emotion Analysis Software*: *Choose How You Feel; You Have Seven Options*, Institute of Network Cultures, 2017. Disponível em: <https://networkcultures.org/longform/2017/01/25/choose-how-you-feel-you-have-seven-options/>. Acesso em 21 nov. 2022.

VARON, Joana; TEIXEIRA, Lucas. *Podemos vigiar os vigilantes?* Coding Rights, 2018, Boletim Antiviligância nº 16, 2018. Disponível em: <https://medium.com/codingrights/podemos-vigiar-os-vigilantes-ac3fe77e7694>. Acesso em 22 dez. 2022.

VASCONCELOS, Beatriz et al. *Neurocientistas defendem limites legais para neuromarketing:* Temor é que a estratégia possa ser usada para manipular o consumidor, publicado em 24 nov. 2021. Disponível em: <https://www1.folha.uol.com.br/especial/2021/11/neurocientistas-defendem-limites-legais-para-neuromarketing.shtml>. Acesso em 23 nov. 2022.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel et al. (coord.). *Tratado de Proteção de Dados Pessoais*, 2ª ed., Rio de Janeiro: Forense, 2023.

WANG, Ying J.; MINOR, Michael S. *Validity, Reliability and Applicability of Psychophysiolgical Techniques in Marketing Research*, Psychology & Marketing, v. 25, n. 2, 2008, pp. 197-232; PLASSMANN, Hilke; RAMSØY, Thomas Z., MILOSAVLJEVIC, Milica. Faculty and Research Working Paper: Branding the Brain: A Critical Review. *INSEAD The Business School of the World*, n. 15/MKT, 2011.

WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*, Harvard Law Review, 4/5, 1890.

WATSON, John B. A psicologia como o behaviorista a vê, *Temas em Psicologia*, vol. 16, n. 2, pp. 289-301, 2008.

WU, Tim. *The attention merchants*: the epic scramble to get inside our heads. New York, Kopf, 2016.

YEUNG, Karen. *Hypernudge*: Big Data as a mode of regulation by design, Information, Communication and Society, v. 10, n.1, pp. 118-136, 2016.

ZANATTA, Rafael. A. F.; ABRAMOVAY, Ricardo. *Dados, vícios e concorrência: repensando o jogo das economias digitais*. Estudos Avançados, [S. l.], v. 33, n. 96, 2019.

_____. *Perfilização, Discriminação e Direitos*: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, 2019, p. 2. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 16 de nov. de 2022.
SUSSER, Daniel; ROESSLER, Beate; NISSENBAUM, Helen. *Online Manipulation:* Hidden Influences in a Digital World, 4 Geo. L. Tech. Rev. 1, 2019.

ZINGALES, L.; ROLNIK, G.; LANCIERI, F. M. Final Report, Stigler Committee on Digital Platforms, *Stigler Center for the Study of the Economy and the State*, 2019.

ZUBOFF, Shoshana. Big Other: surveillance capitalism and prospects of an information civilization. *Journal of Information Technology*, v.30, n.1, pp. 75-89, 2015.

_____. *The age of surveillance capitalism.* The fight for a human future at the new frontier of power. New York: Public Affairs, 2019.

_____. The secrets of surveillance capitalism, *Frankfurter Allgemeine Zeitung*, 2016.

Autoridad Nacional de Protección de Datos Personales multa a financiera y a aseguradora oncológica por llamadas sin consentimento, Gob.pe, publicado em: 14 dez. 2021. Disponível em: <https://www.gob.pe/institucion/minjus/noticias/569980-autoridad-nacional-de-proteccion-de-datos-personales-multa-a-financiera-y-a-aseguradora-oncologica-por-llamadas-sin-consentimiento>. Acesso em 15 jan. 2023.

Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial: Secretaria Nacional do Consumidor condenou a empresa ao pagamento de multa de R$ 58,7 mil por violações ao CDC. Disponível em: <https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial>. Acesso em 12 dez. 2022.

Data Selfie segue todos os seus passos no Facebook. Disponível em: <https://www.techtudo.com.br/tudo-sobre/data-selfie/>. Acesso em: 22 dez. 2022.

Facebook é condenado a pagar R$ 6,6 mi por vazar dados de usuários, Ministério da Justiça e Segurança Pública, 23 ago. 2022. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/facebook-e-condenado-a-pagar-r-6-6-mi-por-vazar-dados-de-usuarios>. Acesso em 17 jan. 2023.

Facebook Political Ad Collector: How Political Advertisers Target You. Disponível em: <https://projects.propublica.org/facebook-ads/>. Acesso em: 22 dez. 2022.

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did. Disponível em: <https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=4ccdae5b6668>. Acesso em 12 dez. 2022.

Idec vai à Justiça contra coleta de emoções de usuários do metrô de SP, Idec, publicado em: ago. 2018. Disponível em: <https://idec.org.br/noticia/idec-vai-justica-contra-coleta-de-emocoes-de-usuarios-do-metro-de-sp>. Acesso em 15 jan. 2023.

Make an accessible framework so anyone can analyze Facebook's newsfeed algorithm. Disponível em: <https://facebook.tracking.exposed/>. Acesso em 22 dez. 2022.

MJSP multa Facebook em R$ 6,6 milhões, Ministério da Justiça e Segurança Pública, 30 dez. 2019. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-multa-facebook-em-r-6-6-milhoes>. Acesso em 17 jan. 2023.

Privacy Badger is a browser extension that automatically learns to block invisible trackers. Disponível em: <https://privacybadger.org/>. Acesso em: 22 dez. 2022.

Projeto Eleições Sem Fake. Disponível em: <https://www.eleicoes-sem-fake.dcc.ufmg.br/>. Acesso em 22 dez. 2022.

Rappi multada por violar protección de datos personales, El Tiempo, 03 nov. 2021. Disponível em: <https://www.eltiempo.com/economia/empresas/rappi-multada-por-violar-proteccion-de-datos-personales-628739>. Acesso em 17 jan. 2023.

Seguradora e financiadora utilizam, sem autorização, dados pessoais para telemarketing publicitário, Construindo Pontes, 2021. Disponível em: <https://construindopontes.org.br/casos/seguradora-e-financiadora-utilizam-sem-autorizacao-dados-pessoais-para-telemarketing-publicitario/>. Acesso em 15 jan. 2023.

Who Targets Me. Disponível em: <https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search/items/who-targets-me.html>. Acesso em: 22 dez. 2022.