UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

JANAINA VIEIRA HOMCI

OS LIMITES DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS DE CONSUMO

BELÉM
2021

JANAINA VIEIRA HOMCI

OS LIMITES DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS DE CONSUMO

Dissertação apresentada à Banca Avaliadora como requisito para a obtenção do título de Mestre pelo Programa de Pós-Graduação em Direito da Universidade Federal do Pará, na linha de pesquisa "Direitos Fundamentais, Concretização e Garantias", área de concentração "Consumo, Cidadania e Solidariedade".

Orientador: Prof. Dr. Dennis Verbicaro Soares

BELÉM
2021

JANAINA VIEIRA HOMCI

OS LIMITES DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS DE CONSUMO

Dissertação apresentada à Banca Avaliadora como requisito para a obtenção do título de Mestre pelo Programa de Pós-Graduação em Direito da Universidade Federal do Pará, na linha de pesquisa "Direitos Fundamentais, Concretização e Garantias", área de concentração "Consumo, Cidadania e Solidariedade".

Aprovado em: 18.08.2021.

Com menção: Aprovado com recomendação de publicação.

Banca Examinadora:

_____

Professor Dennis Verbicaro Soares
Doutor em Direito do Consumidor (Universidad de Salamanca)
Universidade Federal do Pará
Orientador

_____

Professor Ney Stany Morais Maranhão
Doutor em Direito do Trabalho (Universidade de São Paulo)
Universidade Federal do Pará
Examinador interno

_____

Professor Oscar Ivan Prux
Doutor em Direito das Relações Sociais (Pontifícia Universidade Católica de São Paulo)
Universidade Cesumar (PR)
Examinador externo

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

H763l Homci, Janaina Vieira.
Os Limites do Consentimento na Proteção de Dados Pessoais de Consumo / Janaina Vieira Homci. — 2021.
183 f. : il.

Orientador(a): Prof. Dr. Dennis Verbicaro
Dissertação (Mestrado) - Universidade Federal do Pará, Instituto de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Belém, 2021.

1. Dados Pessoais. 2. Vulnerabilidade. 3. Privacidade. 4. Consentimento . 5. Prevenção. I. Título.

CDD 342.5

“Enxergo bem o mundo que quero para todas as crianças, inclusive as minhas. Minha maior esperança é que meu filho e minha filha possam escolher o que fazer com suas vidas sem obstáculos internos ou externos que os atrapalhem ou os levem a questionar suas escolhas.”

Sheryl Sandberg

AGRADECIMENTOS

"Tudo que nóis tem é nóis" já diz a música de autoria do *rapper* Emicida. Tal frase fez-me refletir nos últimos dias de pesquisa e na finalização da dissertação. Embora o mestrado seja uma atividade desenvolvida de forma individual, não conseguiria avançar e, consequentemente, findar, sem o apoio, o alento e a força das pessoas queridas que me rodeiam, especialmente durante a crise instaurada pela pandemia de Covid-19.

Foram incontáveis sorrisos e incansáveis choros nos últimos dois anos, sempre com uma voz amiga ao lado. O sentimento que descreve esta pesquisa, sem dúvida, é gratidão aos meus pais, aos meus amigos e amigas, professores e professoras, orientador e noivo.

Antonio e Antonia, obrigada por acreditar, ouvir, torcer e sonhar junto comigo. Vocês são minha base, minha força e meu maior orgulho na vida. Pai, agradeço pelo constante interesse na pesquisa e nos meus textos, mesmo não sendo da sua área de formação. Seu entusiasmo anima-me a seguir e a avançar na academia.

Aos professores do Programa de Pós-Graduação em Direito (PPGD) da Universidade Federal do Pará (UFPA), obrigada pelo conhecimento compartilhado. Agradeço especialmente ao meu orientador, Dennis Verbicaro, pelo incentivo, pelo apoio e pelos ensinamentos, inclusive antes mesmo do mestrado, como coordenador do Grupo de Pesquisa "Consumo e Cidadania". Tenho muita admiração profissional e pessoal pelo senhor.

Obrigada ao Grupo de Pesquisa "Consumo e Cidadania" e a todos os seus integrantes. É inegável que o resultado deste trabalho também é fruto das discussões realizadas nas reuniões nos últimos quatro anos.

Aos amigos e amigas, obrigada! Debora Vieira, Shayane Paixão e Gabriela Ohana, vocês não imaginam quão brilhantes são. Tenho muito orgulho de trilhar o caminho da pesquisa com vocês.

Aos colegas de turma obrigatória TD(H), agradeço pela leveza e pela alegria. Nossas disciplinas obrigatórias foram mais tranquilas graças ao apoio de vocês.

Aos meus colegas de trabalho, especialmente às amigas Camilla Uliana, Andrea Puget e ao amigo Diego Alves, obrigada pela paciência e pelo incentivo.

Por fim, dedico esta obra ao meu futuro marido Arthur Laércio Homci. Você alegra minha vida, traz luz aos dias difíceis e faz-me ser uma pessoa melhor.

Concluo minha dissertação com inquietação interna, na vontade de produzir mais e na esperança de dias melhores, amparados pela pesquisa brasileira.

“E, quando for fazer compras, adquira uma câmara portátil e um microfone, grave tudo o que você faz e ponha na rede. Permita que o Google e o Facebook leiam todos os seus e-mails, monitorem todos os seus bate-papos e mensagens e mantenham um registro de todas as curtidas e cliques. Se fizer tudo isso, então os grandes algoritmos da internet de todas as coisas lhe dirão com quem casar, que carreira seguir e se é para começar uma guerra.”

Yuval Noah Harari

RESUMO

Os avanços da tecnologia da informação transformaram a relação consumerista. Antes centrada nas figuras do consumidor e do fornecedor na ação direta, seja na compra de um produto, seja na contratação de um serviço, essa relação teve seus agentes reconfigurados pela própria estrutura mercadológica da economia de dados pessoais. Com suas informações pessoais, o destinatário final torna-se a matéria-prima, uma vez que a coleta, o tratamento e a utilização de dados pessoais direcionam o mercado publicitário e, consequentemente, o assédio de consumo. A assimetria relacional, expressa nas vulnerabilidades observadas nesse contexto, altera o sentido do consentimento. Embora não seja a única base autorizativa admitida para o tratamento de dados pessoais, o consentimento sofre limitações, o que suscita a busca da efetiva proteção do consumidor inserido nesse contexto. Esta pesquisa tem duas partes bem definidas: uma destina-se ao diagnóstico da relação de consumo de dados pessoais, analisando desde aspectos objetivos do tratamento de dados em si até os direitos do consumidor, especialmente o reconhecimento da(s) vulnerabilidade(s), a multiformidade do conceito da privacidade, a autonomia de vontade, a proteção de dados pessoais como direito fundamental e a liberdade; a outra examina, à luz do diálogo entre as fontes – o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais –, a responsabilização pelo uso indevido de dados e, diante da caracterização do estado de danosidade, a tutela preventiva por meio do compartilhamento da autoridade política. Destaque é dado ao empoderamento, à atuação ora mediadora, ora punitiva do Estado e à formulação de uma política de governança pelos fornecedores, especialmente em observância ao *compliance*, ao *privacy by design* e à *accountability*. Constata-se que a legislação estabelece um ambiente solidário para uma arquitetura de rede com estratégias tecnológicas e de regulação cujo elemento central é a privacidade.

Palavras-chave: Dados pessoais. Vulnerabilidade. Privacidade. Consentimento. Prevenção.

ABSTRACT

Advances in information technology have transformed the consumer relationship. Before centered on the figures of the consumer and the supplier in direct action, whether in the purchase of a product or in the contracting of a service, this relationship had its agents reconfigured by the market structure of the economy of personal data. With your personal information, the final recipient becomes the raw material, since the collection, processing and use of personal data drive the advertising market and, consequently, consumer harassment. Relational asymmetry, expressed in the vulnerabilities observed in this context, alters the meaning of consent. Although it is not the only authorized basis for the processing of personal data, consent is subject to limitations, which prompts the search for effective consumer protection in this context. his research has two well-defined parts: one is aimed at diagnosing the consumption relationship of personal data, analyzing from objective aspects of data processing itself to consumer rights, especially the recognition of vulnerability(s), the multiformity of the concept of privacy, autonomy of will, protection of personal data as a fundamental right and freedom; the other examines, in light of the dialogue between the sources - the Consumer Defense Code and the General Law for the Protection of Personal Data -, the responsibility for the misuse of data and, given the characterization of the state of damage, the preventive protection by through sharing political authority. Emphasis is given to empowerment, sometimes mediating and sometimes punitive actions of the State and the formulation of a governance policy by suppliers, especially in compliance with compliance, privacy by design and accountability. It appears that the legislation establishes a solidary environment for a network architecture with technological and regulatory strategies whose central element is privacy.

Keywords: Personal data. Vulnerability. Privacy. Consent. Prevention.

LISTA DE FIGURAS

Figura 1 – *Business Intelligence* por meio do DW.
Figura 2 – Ciclo mercadológico por meio de *data brokers*.
Figura 3 – Estratégia de projeto de privacidade.
Figura 4 – Exemplos de PETs conforme sua funcionalidade.

LISTA DE TABELAS

Tabela 1 – Critérios de consentimento.
Tabela 2 – Comparação: CDC *versus* LGPD.
Tabela 3 – Comparação entre artigos da LGPD.
Tabela 4 – Comparação: CDC *versus* LGPD.
Tabela 5 – ANPD na Argentina.
Tabela 6 – ANPD na Colômbia.
Tabela 7 – ANPD no Uruguai.
Tabela 8 – Diretrizes baseadas no Guia sobre PbD da Agência Espanhola de Proteção de Dados Pessoais.

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADI	Ação Direta de Inconstitucionalidade
AEPD	Agência Espanhola de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
Cade	Conselho Administrativo de Defesa Econômica
CC	Código Civil
CDC	Código de Defesa do Consumidor
CENP	Conselho Executivo de Normas-Padrão
CF	Constituição Federal
CNPDP	Conselho Nacional de Proteção de Dados e Privacidade
Conar	Conselho Nacional de Autorregulamentação Publicitária
CVM	Comissão de Valores Mobiliários
DCU	*Design* centrado no usuário
DNT	*Do Not Track*
DSP	*Demand-Side Platforms*
DW	*Data Warehousing*
Enisa	Agência Europeia para a Segurança das Redes e da Informação Segurança
EUA	Estados Unidos da América
FB	Facebook Inc.
FTC	Federal Trade Commission
IBGE	Instituto Brasileiro de Geografia e Estatística
Idec	Instituto Brasileiro de Defesa do Consumidor
IP	*Internet Protocol*
LCP	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados
Metux	*Motivation, Engagement and Thriving in User Experience*
MP	Medida Provisória
OCDE	Organização para a Cooperação e o Desenvolvimento Econômico
OLAP	*Online Analytical Processing*

OPC	Office of the Privacy Commissioner
PbD	*Privacy by design*
PETs	*Privacy enhancing technologies*
PEPP-PT	*Pan-European Privacy-Preserving Proximity Tracing*
PIA	*Privacy impact assessment*
PL	Projeto de Lei
PLL	*PrimeLife Policy Language*
PNRC	Política Nacional das Relações de Consumo
PNPDPP	Política Nacional de Proteção de Dados e Privacidade
P3P	*Platform for Privacy Preferences Project*
RTB	*Real Time Bidding*
SDT	*self-determination theory*
Senacon	Secretaria Nacional do Consumidor
SIC	Superintendência de Indústria e Comércio
Sindec	Sistema Nacional de Informações de Defesa do Consumidor
SSP	*Supply-Side Platforms*
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCP	*Transmission Control Protocol*
XACML	*eXtensible Access Control Markup Language*

SUMÁRIO

1	**INTRODUÇÃO**	**14**
2	**ECONOMIA DE DADOS E CONSUMO: ENTRE A VIGILÂNCIA E O CONTROLE**	**19**
2.1	**Os dados dos consumidores como** um **ativo na economia: formas de coleta, tratamento e circulação**	**28**
2.2	**O novo modelo de negócio *on-line*: o *microtargeting***	**33**
2.2.1	*Geoblocking* e *geopricing* como ferramentas de *microtargeting*	34
2.3	**A publicidade como veículo pré-contratual e sua nova dimensão no ambiente virtual**	**36**
2.3.1	Publicidade direcionada: contextual, segmental e comportamental	40
2.3.2	Assédio de consumo *on-line* na publicidade direcionada	42
2.4	**A reconfiguração dos atores que compõem a publicidade direcionada: o novo consumidor e o fornecedor**	**44**
3	***E-COMMERCE*, DADOS PESSOAIS E RELAÇÕES DE CONSUMO: UMA ANÁLISE DAS CARACTERÍSTICAS DO CONSUMO NO COMÉRCIO ELETRÔNICO**	**48**
3.1	**A vulnerabilidade do consumidor agravada na contratação eletrônica e na economia de dados pessoais**	**55**
3.1.1	A vulnerabilidade informacional do consumidor na economia de dados pessoais	60
3.1.2	A vulnerabilidade psicocomportamental	64
3.1.3	A nova dimensão da vulnerabilidade situacional do consumidor	67
3.1.4	A vulnerabilidade algorítmica na assimetria de controle e informação	68
3.2	**Privacidade: um conceito multiforme**	**70**
3.2.1	A proteção dos dados pessoais como direito autônomo e fundamental	77
3.2.2	A autodeterminação informativa	82
3.2.3	Privacidade contextual: a integridade e o contexto na construção de normas informacionais	84
3.3	**A relativização da liberdade e o exercício da autodeterminação informativ**a	**86**
4	**O PAPEL DO CONSENTIMENTO NA PROTEÇÃO DE DADOS DE CONSUMO**	**89**
4.1	**Bases legais autorizadoras do tratamento de dados pessoais**	**89**
4.2	**O consentimento e sua função na economia de dados pessoais**	**91**
4.3	**O diálogo das fontes: a Lei Geral de Proteção de Dados (Lei n.° 13.709/2018) e o Código de Defesa do Consumidor (Lei n.° 8.078/1990)**	**96**
4.3.1	A caracterização do consentimento ativo à luz da base principiológica da legislação	98
4.3.2	Responsabilidade civil por uso indevido e irregular de dados	101
4.3.3	Tutela coletiva na proteção de dados de consumo	107
4.4	**Consentimento e responsabilidade civil: entre o dano e o estado de danosidade social**	**111**

5 A CIDADANIA INSTRUMENTAL NA PROTEÇÃO DOS DADOS DOS CONSUMIDORES: O COMPARTILHAMENTO DA AUTORIDADE ENTRE OS AGENTES DA RELAÇÃO 114
5.1 O consumidor e o seu empoderamento no ambiente virtual 116
5.1.1 O paradoxo entre o consumidor de vidro e o consumidor identitário no contexto pandêmico 119
5.2 O papel mediador do Estado na proteção de dados de consumo 121
5.2.1 Autoridade Nacional de Proteção de Dados 121
5.2.2 Política Nacional de Proteção de Dados Pessoais e da Privacidade 129
5.3 Controle dos *gatekeepers*: aspectos preventivos e estruturais 132
5.3.1 Governança, boas práticas e *compliance* 133
5.3.2 *Design* e *privacy by design*: a proteção da privacidade do usuário/consumidor como elemento central da construção de estratégias tecnológicas 136
5.3.2.1 *Privacy Enhancing Technologies* na concretização do *privacy by design* 143
5.4 Regulação e *accountability* na economia de dados 146

6 CONCLUSÃO 154

REFERÊNCIAS 160

1 INTRODUÇÃO

A revolução tecnológica e o consequente estabelecimento da sociedade de informação exigiram a modificação do consumo, que passou a ser feito em relações desmaterializadas, desterritorializadas e, em princípio, despersonalizadas[1]. O capitalismo, em que a informação é o eixo da formulação de produtos e serviços, impôs práticas direcionadas para a redução dos custos mercadológicos e, por conseguinte, para o aumento do valor do negócio. Assim, os dados pessoais tornaram-se um dos principais ativos do capitalismo informacional, tendo como principal motor o *Big Data*.

Para Zuboff (2018), implantou-se um capitalismo de vigilância, que exige uma nova forma de poder, a qual, suplantada pelas punições e pelas premiações de uma mão invisível, solapa o contrato e o Estado de Direito:

> O capitalismo de vigilância, portanto, se qualifica como uma nova lógica de acumulação, com uma nova política e relações sociais que substituem os contratos, o estado de direito e a confiança social pela soberania do *Big Other*. Ele impõe um regime de conformidade baseado em recompensas e punições e administrado privadamente, sustentado por uma redistribuição unilateral de direitos. O *Big Other* existe na ausência de uma autoridade legítima e é em grande parte livre de detecção ou de sanções. Neste sentido, o *Big Other* pode ser descrito como um golpe automatizado de cima: não um *coup d'État*, mas sim um *coup des gens* (ZUBOFF, 2018, p. 49).

A pandemia de Covid-19 expôs com mais intensidade a necessidade de proteção dos dados pessoais em todos os níveis. Diversos países, inclusive o Brasil, estão utilizando dados, agregados e/ou individualizados, para implantar políticas de combate a essa doença. De acordo com a teoria de Agamben (2007), vive-se num estado de exceção, em que se fixou um limiar de indiscernibilidade para a proteção da privacidade diante da necessidade de combate à doença e do interesse público em que pairam os dados pessoais no país.

Pode-se ainda destacar que, em razão da utilização dos dados pessoais nas políticas de combate da pandemia e da própria crise política instaurada no país em 2020, vive-se em um marco histórico para a área da privacidade e a proteção de dados diante de tantas discussões[2] no Supremo Tribunal Federal (STF) sobre a temática.

---

[1] Para Marques (2004a), mesmo com o direcionamento publicitário, as relações no *e-commerce* são despersonalizadas principalmente em razão do contrato de adesão. Para outras partes da doutrina, como Bioni (2019, 2020a), Doneda (2019) e Mendes (2019), a publicidade direcionada é consequência da individualização e da personificação do mercado diante do acesso, do tratamento e da disposição de dados pessoais pelo *Big Data*.

[2] *Fake news*, marco civil da internet, sigilo e criptografia têm tomado conta das discussões do STF. Destaca-se a decisão histórica proferida pelo STF ao reconhecer, nos dias 6 e 7 de maio de 2020, um direito fundamental autônomo à proteção de dados pessoais. O julgamento do plenário referendou a Medida Cautelar nas Ações Diretas de Inconstitucionalidade (ADI) n.º 6387, n.º 6388, n.º 6389, n.º 6393 e n.º 6390, para suspender a MP n.º 954/2018,

O *Big Data*, nesse sentido, possibilitou a formulação de perfis comportamentais dos usuários por meio de técnicas de coleta, tratamento e disponibilização de dados pessoais, o que inegavelmente facilitou o controle difuso e individual. Segundo Lace (2005), o consumidor transformou-se em um consumidor de vidro, ou seja, aquele cujos gostos, predileções e ações são facilmente identificados pelo acesso a seus dados pessoais. As empresas utilizam essas informações como matéria-prima para a produção de seus produtos e serviços; observam o mercado, produzem e direcionam seus produtos ao público-alvo por meio da publicidade direcionada comportamental, segmental e contextual. Mais ainda, seus produtos são identificados aos destinatários finais por meio de técnicas chamadas *microtargeting*.

Nesse aspecto, é importante frisar a utilização de técnicas de *geopricing* e *geoblocking* na segmentação do consumidor, as quais, por meio do assédio de consumo, visam não apenas persuadi-lo, mas também modular o seu comportamento, o que reconfigura as dimensões conceituais do consumidor, como matéria-prima e destinatário final, e fornecedor, sendo todos os atores envolvidos na prática do negócio com ganhos diretos e indiretos.

Tais técnicas, quando não autorizadas de forma ativa com base em informações que possibilitem o verdadeiro exercício da vontade, são violadoras de direitos fundamentais, especialmente no que concerne à vulnerabilidade e à privacidade.

No que diz respeito à vulnerabilidade, é fato que as próprias características da contratação virtual agravam a vulnerabilidade do consumidor inserido no contexto de tratamento de dados pessoais. Por outro lado, a associação das características da contratação eletrônica com as assimetrias relacionais do mercado informacional agrava ainda mais tal vulnerabilidade, possibilitando a identificação de novas categorias, especialmente a informacional, a psicocomportamental, a situacional e a algorítmica.

A especificação do princípio da vulnerabilidade do consumidor não se limita a categorizar, visa diagnosticar tendo em vista a responsabilização por uso indevido de dados pessoais e o estabelecimento de práticas preventivas.

Quanto à privacidade, em sentido individual e coletivo, há um concreto desrespeito a tal direito que atinge o direito negativo (direito ao sigilo, ao segredo, à interferência de terceiros e a estar só) e o direito positivo por meio do controle das informações pessoais. Nesse caso, vale frisar o estabelecimento do direito fundamental e autônomo à proteção de dados pessoais pelo exercício da autodeterminação informativa, seja por meio do consentimento, acesso às informações pessoais e do exercício da cidadania instrumental.

---

que obrigava as operadoras de telefonia a repassarem ao Instituto Brasileiro de Geografia e Estatística (IBGE) dados pessoais individualizados dos consumidores, como celular e endereço (MENDES, 2020a).

Assim, em consonância com esse contexto, os dados pessoais alimentam as relações de consumo no ciberespaço, mecanismos de assédio de consumo por publicidade direcionada continuam a ser usados com base no consentimento involuntário. Considerando a responsabilização por dano estipulada nas legislações pertinentes, questiona-se: como proteger a privacidade do consumidor diante da publicidade direcionada pela modulação algorítmica de dados pessoais?

Quando se fala da importância do consentimento na relação de consumo de dados, é necessário destacar o diálogo das fontes, em uma relação de complementaridade e de subsidiariedade, entre a LGPD – Lei n.º 13.708/2018 – e o Código de Defesa do Consumidor (CDC) – Lei n.º 8.078/1990, especialmente no que diz respeito à imputação do direito-dever à informação. Frisa-se ainda a interpretação sistêmica da caracterização da responsabilidade civil e de suas excludentes, seja no aspecto individual, seja no aspecto coletivo, em atenção à punição do dano e à realização de práticas com base no princípio da segurança a fim de evitar o estabelecimento do estado de danosidade.

Não se exclui a importância da responsabilidade civil pela incidência de dano em razão do uso indevido de dados, mas constata-se sua insuficiência protetiva diante da complexidade do contexto apresentado. Assim, sob o prisma preventivo, visa-se o estabelecimento do compartilhamento da autoridade política por meio da cidadania instrumental e da atuação conjunta dos agentes na busca do equilíbrio mercadológico.

Cumpre destacar o empoderamento do consumidor e sua atuação emancipatória e contrária às imposições do mercado, atentando ao consumo identitário exacerbado durante a crise pandêmica.

O Estado, por sua vez, atua sob uma perspectiva binária, ora sendo mediador entre os agentes, ora fazendo uso do poder fiscalizatório e punitivo. Ressalta-se a atuação fiscalizatória e orientadora da Autoridade Nacional de Proteção de Dados (ANPD) no incentivo à governança.

O fornecedor, por fim, deve adotar práticas que ensejam a prevenção e a segurança desde a concepção do produto ou serviço, por meio de regras de *compliance* e/ou estruturais, como a adoção do *privacy by design* (PbD). Com efeito, a prevenção de danos por meio da proteção da privacidade é o centro do desenvolvimento do produto e/ou serviço, os riscos e liberdades do titular de dados e a segurança da informação, para evitar a exposição danosa reputacional diante da incidência da prestação de contas (*accountability)*.

Esta pesquisa tem por objetivo analisar como a publicidade direcionada pela modulação algorítmica na economia de dados agrava a vulnerabilidade do consumidor em razão do

desrespeito à sua privacidade, no âmbito individual e coletivo. Diante da atual assimetria de poder e de informação, atingir esse objetivo exige a busca de um novo mecanismo de proteção. Para isso, recorre-se inicialmente ao estudo doutrinário dos referenciais teóricos selecionados como guias de análise do problema, com uma análise interdisciplinar que envolve a filosofia, o direito do consumidor, o direito regulatório, o *design* e a tecnologia de informação, por meio do método dedutivo.

No campo da economia de dados, das relações de poder e de consumo, toma-se como base o estudo filosófico da economia de dados como uma relação de poder, na qual o consumo se torna o condutor central do indivíduo e a publicidade é um dos principais eixos.

Por outro lado, foi necessário recorrer à tecnologia da informação para analisar os mecanismos de coleta, tratamento e disposição de dados pessoais e examinar a formação de um novo ciclo mercadológico com novos agentes inseridos, a fim de demonstrar suas marcas centrais e identificar como a publicidade ganhou uma nova dimensão, a partir de uma reconstrução direcionada, possibilitando a incidência do assédio de consumo no ambiente virtual.

A análise das características da contratação eletrônica permite constatar a vulnerabilidade do consumidor inserido nesse contexto, bem como a multiformidade da privacidade no mercado informacional. Visa-se comprovar desse modo a viabilidade do consentimento ativo na relação em discussão.

A análise bibliográfica, portanto, constitui a base da primeira e da segunda parte da pesquisa a ser desenvolvida. Em um terceiro momento, chega-se à análise legislativa, considerando principalmente o diálogo das fontes, o diálogo entre a LGPD – Lei n.º 13.709/2018 – e o CDC – Lei n.º 8.078/1990, na caracterização do consentimento ativo, da responsabilidade civil e da tutela coletiva.

Por fim, analisa-se o compartilhamento da autoridade política na realização da cidadania instrumental de modo a colocar em prática condutas preventivas por parte dos agentes tendo em vista o equilíbrio mercadológico. Busca-se, assim, mensurar o possível aprimoramento e a expansão da proteção de dados pessoais dos consumidores inseridos na economia de dados a partir do seu empoderamento e da atuação punitiva e mediadora do Estado. Por outro lado, busca-se examinar a implementação da governança, do *compliance*, da metodologia com base no *design* e na tecnologia da informação a fim de demonstrar uma arquitetura de rede centrada no usuário com objetivo de estabelecer o direito à transparência e do direito-dever à informação, além de outras direitos mencionados ao longo do estudo.

Por tudo, a pesquisa visa superar a mera dogmática jurídica, buscando na filosofia, no direito, na tecnologia da informação e no *design* respostas práticas para a proteção do consumidor.

2 ECONOMIA DE DADOS E CONSUMO: ENTRE A VIGILÂNCIA E O CONTROLE

O poder é relacional e é exercido sobre cada indivíduo por meio de mecanismos de controle (BAZZICALUPO, 2017). Para Foucault (1999), o poder divide, ordena, coordena e está tão presente nas vidas que se torna imperceptível.

Em linhas gerais, o poder soberano é exercido sobre o território, nos seus limites e nas suas fronteiras. Dentro da territorialidade, o soberano poderá determinar qual lei impera e qual punição será imposta em caso de desobediência. Para Schmitt (2005), o soberano é quem decide pelo estado de exceção e, com base nessa decisão, reinstaura a ordem pela vigência do caos. Divergindo desse entendimento, Agamben (2007) afirma que se vive em um constante estado de exceção pelo estabelecimento de um limiar de indiscernibilidade: todos estão incluídos no sistema e todos são excluídos do sistema, ou seja, todos são chamados a ser um *Homo sacer*, vários entes exercendo essa força de controle subjetiva, como o capital (AGAMBEN, 2007).

De acordo com a teoria foucaultiana, entre o século XVIII e o XIX, houve a transição do poder soberano para o poder disciplinar. Isso se deveu em parte ao surgimento de clínicas psiquiátricas e à "humanização" das prisões (BAZZICALUPO, 2017). O poder deixou de fixar a lei e passou a focar a internalização subjetiva da norma, "através de mecanismos de dominação do corpo social, que os [*sic*] mantinha atado por uma trama cerrada de coerções disciplinares, de forma a garantir-lhe coesão" (MALCHER; DELUCHEY, 2016, p. 43). O poder disciplinar, portanto, usa como instrumento uma hierarquia clara, uma série de atividades repetitivas, vigilância e avaliação para formar corpos dóceis. A identidade torna-se uma imposição do Estado, ou seja, é ensinada por fórmulas gerais de dominação.

São técnicas de controle dos corpos, sobre produtos de trabalho e rituais de obediência, que realizam uma constante força tendo em vista a submissão. Para Foucault (1999, p. 189), "a disciplina não é mais simplesmente uma arte de repartir os corpos, de extrair e acumular o tempo deles, mas de compor forças para obter um aparelho eficiente". O poder disciplinar não tem a função de se apropriar, mas de adestrar, e a vigilância torna-se um operador econômico decisivo por ser peça interna do aparelho de produção e da engrenagem do poder disciplinar. O modelo pan-óptico proposto por Bentham é descrito por Foucault (1999, p. 223):

> O *Panóptico* de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar.

Trata-se de uma forma de assujeitamento dos presos uma vez que, entendendo que são observados, agem de forma pacífica, independentemente da comprovação da vigilância, pelo simples temor da observação. Assim, o controle é realizado de maneira subjetiva e individual, cada pessoa sendo vigiada de acordo com as normas estipuladas no estabelecimento.

O surgimento da sociedade disciplinar é reflexo do estabelecimento do poder disciplinar, cujo modelo é o esquema pan-óptico. Não há a substituição de um poder por outro, há a infiltração da modalidade disciplinar em todas as outras, "servindo-lhes de intermediária, ligando-as entre si, prolongando-as, e principalmente permitindo conduzir os efeitos de poder até os elementos mais tênues e mais longínquos" (FOUCAULT, 1999, p. 239). Nessa lógica, a norma, em sentido amplo, é muito importante para integrar os indivíduos à sociedade, caso contrário, seriam excluídos. Aqueles que facilmente se moldassem à norma seriam recompensados. Pode-se afirmar, portanto, que a sociedade disciplinar caracterizou-se por técnicas de modulação subjetiva para o exercício do controle pela imposição da servidão voluntária[3] (LA BOÉTIE, 2016) dos indivíduos em razão da constante possibilidade de exclusão.

Por outro lado, a biopolítica e o biopoder surgem com o enfraquecimento do poder soberano, como uma nova forma de controle da vida por meio da gerência biológica: "questões como as do nascimento e da mortalidade, do nível de vida e da duração da vida estão ligadas não apenas a um poder disciplinar, mas a um tipo de poder que se exerce no âmbito da espécie, da população, com o objetivo de gerir a vida" (FOUCAULT, 2015, p. 29).

Para Fachini e Ferrer (2019), biopolítica e o biopoder ligam-se à tecnologia moderna para exercer o controle da vida. Os indivíduos deixam-se ser dominados pela sedução realizada pelas tecnologias, que camuflam a realidade e exercem uma vigilância hierarquizada. Trata-se de uma "mão invisível, movida pelo governo e pelo comércio, [que] está criando uma arquitetura que vai aperfeiçoar o controle e possibilitar uma regulação altamente eficiente" (LESSIG, 2006, p. 4, tradução nossa)[4].

Nesse sentido, Cassino (2018) afirma que se passou da tipificação da sociedade disciplinar, estabelecida por Foucault, para a sociedade de controle, cuja ferramenta é a modulação[5] pela tecnologia. Na sociedade de controle, o mundo do trabalho mudou

[3] Servidão voluntária é um termo utilizado por Étienne de la Boétie para expressar os motivos pelos quais os indivíduos preferem seguir regras determinadas por tiranos a exercer sua própria liberdade. Na modernidade, tal servidão pode ser relacionada aos dispositivos que aniquilam o homem, como as práticas mercadológicas de persuasão ao consumo.

[4] No original: "This invisible hand, pushed by government and by commerce, is constructing an architecture that will perfect control and make highly efficient regulation possible".

[5] A sociedade de controle tem o poder de modular, de cristalizar uma determinada subjetividade desejada, sendo mais sutil por forjar mecanismos de influência, conforme modelo de Gilles Deleuze (1992).

abruptamente e, considerando ainda a fluidez tecnológica, ocorreu uma crise nos espaços fechados em que se exercia o poder disciplinar. Assim, o exercício do poder passou a se dar em espaços abertos e na mobilidade, operando de forma contínua, em diferentes níveis e o tempo todo.

Para Foucault (2008, p. 369), o poder reproduz não mais o corpo dócil, mas o homem flexível, o sujeito competitivo, o empresário de si mesmo, que tem sua subjetividade produzida pelo neoliberalismo – o *Homo oeconomicus*:

> [...] aquele que aceita a realidade, que responde sistematicamente às modificações nas variáveis do meio, esse *homo oeconomicus* aparece justamente como o que é manejável, o que vai responder sistematicamente a modificações sistemáticas que serão introduzidas artificialmente no meio.

Assim, o *Homo oeconomicus* no âmbito do liberalismo é um sujeito de interesse, governável por observar as possibilidades de sucesso empresarial, cujo capital humano é o trabalho:

> O *homo oeconomicus* em tudo enxerga oportunidade, não se rebela e trabalha ainda mais para consumir. Confinado em sua vida privada, tem em seus interesses particulares o grande norte existencial. Essa sociedade de consumo gerou apatia e confinamento na esfera privada como a única que importa e deve ser legitimada (HOMO..., 2015, p. 1).

Assim, o controle e o monitoramento social são exercidos por taxações biológicas, como mortalidade e natalidade, sendo a governabilidade[6] exercida por qualquer agente econômico que busca a manipulação da vida cotidiana. O desempenho ganha essencial importância para o indivíduo, que deve observar e desenvolver o seu capital humano; o indivíduo torna-se flexível, competitivo e indolente, controlado e facilmente manipulado pelo mercado. No mesmo sentido, Deleuze (1992, p. 222) destaca que a mutação do capitalismo modificou o exercício do poder, o controle é executado de forma contínua e ilimitada, os "indivíduos tornam-se dividuais, divisíveis e as massas tornam-se amostras de dados, mercados ou 'bancos'", sendo o *marketing* instrumento da modulação social.

Para Adriano Correia Silva (HOMO..., 2015), existe uma aproximação conceitual entre o *Homo oeconomicus* de Foucault (2008) e o *Animal laborans* de Arendt (2007) diante do controle da vida pela economia e do conformismo de uma servidão voluntária.

Para Arendt (2007), três atividades humanas expressam a vida ativa, condição básica do homem: o labor, o trabalho e a ação. Labor é a atividade correspondente ao processo biológico do corpo humano, cujo crescimento espontâneo, metabolismo e eventual declínio estão

[6] Diz Foucault (2015, p. 143-144): "por esta palavra, 'governamentalidade', entendo o conjunto constituído pelas instituições, os procedimentos, análises e reflexões, os cálculos e as táticas que permitem exercer essa forma bem específica, embora muito complexa, de poder que tem por alvo principal a população, por principal forma de saber a economia política e por instrumento técnico essencial os dispositivos de segurança".

relacionados com as atividades vitais da própria vida; o trabalho é a atividade de produção da vida artificial das coisas, diferentemente do ambiente natural – *animal laborans*; já a ação está ligada à condição humana de pluralidade e àquilo que diferencia cada um.

O labor e o consumo são dois estágios do processo que impõe ao homem o cumprimento de suas necessidades de vida. No entanto, não significaram a emancipação do homem. O chamado *labor power* designa a mudança de proporção entre o consumo e a labor: o indivíduo deve criar inúmeras oportunidades para manter sua inata capacidade de consumo, marcada pela mecanização e pela artificialização da vida natural; deve ainda criar necessidades artificiais, impostas pelo mercado. A consequência é a universalização da infelicidade e a inconsciência coletiva acerca das exigências mercadológicas, o que caracteriza a chamada sociedade de consumidores (ARENDT, 2007).

Assim, o ponto de convergência entre o *Homo oeconimicus* e o *Animal laborans* é o capital, e o consumo é um dos seus principais eixos. Afirma Adriano Correia Silva:

> Penso ser significativo e digno de reflexão que tanto Arendt quanto Foucault tenham pensado os tempos presentes, no que tange à relação entre economia e política, considerando a centralidade do "consumidor" e da forma de vida que lhe é correlata, assim como que tenham indicado o caráter apolítico e mesmo antipolítico dessa forma de vida (HOMO..., 2015, p. 8).

Consumir passou a ser visto como um investimento em si mesmo e em sua capacidade de suprir a demanda; consequentemente, para continuar ativo, é necessário aceitar as novas tendências impostas pelo mercado sob pena de ser dele excluído. A centralidade do capital impôs a dualidade consumidor-mercadoria pela transformação do ser em ter.

Segundo Silva (2018, p. 114-115), "esse mito do consumo de supérfluos como algo bom e imperdível foi muito bem produzido e difundido pelo capitalismo que necessitava vender sua produção encalhada e fazer o mercado e o capital girarem". O consumismo tornou-se um artifício para movimentar o ciclo financeiro, próprio de um tipo de sociedade que promove, encoraja ou reforça a escolha de um estilo de vida, uma estratégia existencial consumista e rejeita todas as opções culturais alternativas (BAUMAN, 2008).

O indivíduo, nesse contexto, esvai-se diante do maquinário, vê-se, paradoxalmente, dependente dele. Por causa da imensa quantidade de informações direcionadas às massas, há a ilusão de que o espírito desperta; na verdade, o indivíduo idiotiza-se ante o enclausuramento imposto pelos novos padrões, muitos dos quais concebidos para estimular o consumo a partir dos valores projetados pela chamada indústria cultural, que cria modos ideais de vida, impostos na música, na cultura, no cinema, no entretenimento, os quais devem ser seguidos por uma sociedade massificada, padronizada e globalizada. O consumo, portanto, é constitutivo do

reconhecimento social, e a sociedade impõe hábitos comuns em escala global para fomentar a economia capitalista, sua produção e sua lucratividade (VERBICARO; VERBICARO, 2017, p. 112).

Para Lipovetsky (2007), a sociedade de consumo é superada pelo hiperconsumo. De fato, haveria três eras do capitalismo de consumo. A primeira fase é marcada pelo capitalismo de consumo que, por meio de técnicas, possibilitou a produção em massa e, consequentemente, a democratização dos bens de consumo; concentrou-se, porém, na burguesia.

Na segunda fase do capitalismo, o consumo não se vincula a uma classe específica. O crédito permitiu o acesso a demandas materiais, invadindo o cotidiano e ligando-se às necessidades artificiais[7] da coletividade. Trata-se da chamada "sociedade da abundância". Deu-se após a Segunda Guerra Mundial e caracterizou-se pela padronização e pela elevação da produtividade. A automatização das linhas de montagem possibilitou a fabricação de produtos em grandes quantidades, segundo a dita "lógica da quantidade" (LIPOVETSKY, 2007, p. 33).

A revolução tecnológica modificou a própria sociedade e o próprio ato de consumir. Com o seu avanço, produtos da indústria cultural tornam-se pontos de apoio de novas tecnologias intelectuais e imperam por meio de estoques de conhecimentos que estruturam as composições de novos bens e serviços:

> Discos óticos ou programas disponíveis na rede poderão funcionar como verdadeiros kits de simulação, catálogos de mundos que poderão ser explorados empiricamente, através de imagens e sons sintetizados. Os imensos bancos de imagens reunidos pelas companhias de produção cinematográfica e televisivas serão indexados e acessíveis a partir de qualquer terminal da mesma forma que os bancos de dados de hoje. Estas massas de imagens óticas ou simuladas poderão ser filtradas, reempregadas, coladas, desviadas para todos os usos heterodoxos ou sistemáticos imagináveis (LÉVY, 1993, p. 63).

Na chamada sociedade da informação, há uma ênfase nos dispositivos personalizados, na interatividade, na formação de redes e na busca por novas descobertas tecnológicas. A princípio, não combinava com o mundo comercial, tradicional e corporativo. Inconscientemente, a evolução tecnológica da informação foi difundida pela cultura graças ao espírito libertário dos movimentos dos anos 60 do século XX (CASTELLS, 2000).

No primeiro momento, a difusão da internet fez-se sob a ótica da ideologia liberal, herdada da época industrial. Posteriormente, após a década de 70, as transformações na organização da produção foram acompanhadas por representações sociais. A economia do conhecimento e do saber é marcada pela passagem da produção de bens para a prestação de serviços (LOVELUCK, 2015).

---

[7] A necessidade artificial está ligada à satisfação consumista, voltada para a busca da felicidade ou da integração social por meio de bens de consumo.

No mesmo período, o mercado passava por uma transformação estrutural. A produção em massa dava lugar à economia mais especializada na tentativa de criar novos mercados e nichos de consumidores. O foco não era mais a massificação e a padronização, mas a individualização para criar, diversificar e fidelizar os consumidores às marcas. Nesse momento, surge a chamada terceira fase do capitalismo, na qual o consumo se torna uma forma de consolo e funciona como agente de experiências emocionais que valem por si mesmas. Não se trata apenas de vender serviços, mas de vender experiências, ligadas ao inesperado, capazes de causar emoções, afetos, sensações (economia de experiência) e de forma íntima. Vive-se, então, o consumo hedonista, de lazer e da economia da experiência (LIPOVETSKY, 2007). Tal fase está em constante intensificação, atrelada à personalização exacerbada dos bens de consumo, influenciada pelo avanço tecnológico ante o acesso à informação ocorrido nas décadas seguintes.

A partir das décadas de 80 e 90, a rede foi apropriada por diversos grupos e indivíduos com diferentes objetivos. Com a passagem da tecnologia do controle militar para o domínio civil da internet, a sociedade da informação materializou-se em supervias da informação. Paralelamente a esse processo, nota-se o surgimento de outra mídia, baseada na gratuidade e na troca: a arquitetura aberta e a participação ativa dos usuários, de modo que cada um poderia ser produtor e consumidor de informações (LOVELUCK, 2015).

Tal aprimoramento da rede foi essencial para a reestruturação do sistema capitalista. A partir desse período, o desenvolvimento e a manifestação da revolução tecnológica foram moldados pela lógica dos interesses do capitalismo informacional:

> Uma série de reformas, tanto no âmbito das instituições, como no gerenciamento empresarial, visavam quatro objetivos principais: aprofundar a lógica capitalista de busca do lucro nas relações capital-trabalho, aumentar a produtividade do trabalho e do capital; globalizar a produção, circulação de mercados, aproveitando as condições mais vantajosas para a realização de lucros em todos os lugares; e direcionar o apoio estatal para ganhos de produtividade e competitividade das economias nacionais frequentemente em detrimento da proteção social e das normas de interesse público. A inovação tecnológica e a transformação organizacional com enfoque na flexibilidade e na adaptabilidade foram absolutamente cruciais para garantir a velocidade e a eficiência de reestruturação. Pode-se afirmar que, sem a nova tecnologia da informação, o capitalismo global teria uma realidade limitada: gerenciamento flexível teria sido limitado à redução de pessoal, e a nova rodada de gastos, tanto de bens de capital quanto de novos produtos para consumo, não teria sido suficiente para compensar a redução de gastos públicos. Portanto, o informacionalismo está ligado à expansão e ao rejuvenescimento do capitalismo (CASTELLS, 2000, p. 36-37).

Nesse sentido, a redução de custos de transações e a possibilidade de identificar, atingir e entender o consumidor difundiram rapidamente a concepção de que a internet é um mercado desmaterializado e, por isso, ideal pela inexistência de atritos. Daí uma “nova economia”: a

economia de rede, "baseada em uma abolição da distância e feita de preços reduzidos, de ofertas mais diversificadas e personalizadas" (LOVELUCK, 2015, p. 119), sendo a riqueza dependente da inovação perpétua.

Assim, a revolução tecnológica reestruturou a noção de mercado com base na informação. A excessiva produção em massa foi substituída pela realização de serviços mais individualizados e direcionados através da rede. Se Deus não morreu (2012) e se tornou o próprio dinheiro (AGAMBEN, 2007), sem dúvida nenhuma, pode-se afirmar que o exercício do poder está também no capitalismo informacional, e o principal vetor da sociedade da informação é o *Big Data*.

Para Zuboff (2018, 2020), o capitalismo da informação caracteriza-se pela centralidade das informações como matéria-prima mercadológica. Tais informações são obtidas do *Big Data*, que visa uma constante vigilância e um monitoramento individual. Segundo a autora, o capitalismo informativo tornou-se o capitalismo de vigilância pelos contínuos modelos de controle baseados no sistema de tecnologia. Os dados têm essencial importância nesse contexto por serem fonte de abastecimento do *Big Data*, derivados de transações econômicas, de fluxos mediados por computadores, do banco de dados governamentais, corporativos e das câmeras de vigilância públicas[8] e privadas[9]. São construídos perfis detalhados, com finalidade ideológica ou mercadológica. A subjetividade é convertida em objeto, e a liberdade de navegar na internet está em constante reformulação em razão da invasão de privacidade e, consequentemente, da modulação comportamental. A previsibilidade do exercício da vontade dá lugar ao vazio da servidão voluntária eterna.

Para Bauman (2013), esse processo de vigilância e controle realizado no ciberespaço indica a vigência do modelo pós-pan-óptico[10]. Quanto maior o acesso aos dados pessoais, maior será o poder daquele que os detém diante daqueles que os expõem. A inviabilidade do anonimato em razão da condição de confissão e de servidão voluntária da sociedade atual é uma consequência dos serviços realizados na internet e nas mídias sociais. O indivíduo tem papel

[8] O atual cenário de combate à pandemia intensificou o uso dos dados pessoais em âmbito mundial. Estados asiáticos como Japão, Coreia, China, Hong Kong, Taiwan e Singapura têm apostado no *Big Data*. Na China, por exemplo, a busca por possíveis infectados baseia-se somente em dados técnicos, averiguando os que são potenciais infectados e os que precisam ser observados e isolados, inclusive sob a vigilância de câmeras públicas (HAN, 2020).

[9] O Google já foi condenado pela invasão de privacidade pela utilização da tecnologia *street view*, com a publicação da imagem pessoal sem qualquer tipo de ferramenta de despersonalização (GOOGLE..., 2015). Nos Estados Unidos, o Google foi processado porque os veículos usados em seu serviço de mapeamento topográfico podem ter capturado senhas e outras informações de redes domésticas desprotegidas nos lugares por onde passavam. A violação ficou conhecida como *Wi-Spy* (ROSA, 2019).

[10] Vale ressaltar que Bauman (1999) entende que o sinóptico é uma variação do modelo pós-pan-óptico que opera por meio da vigilância em rede pela disposição e pelo acesso a dados pessoais.

ativo na sua própria vigilância, uma vez que responder negativamente aos ditames da sociedade confessional implica a morte social pela exclusão[11]. Além disso, o *Homo oeconomicus* tem necessidade de transformar a sua exposição em capital humano.

Quando se observa tal modelo em confronto com a disposição e o acesso a dados pessoais na rede, é nítido que os conceitos de controle, de disciplina e de poder caminham para uma nova designação, em razão da constante vigilância, e os algoritmos mostrarão aqueles que devem ser confinados, reorientados e excluídos (BAUMAN, 2013) pela sua discriminação racional algorítmica.

O poder é exercido pela vigilância e pelo controle por meio do conhecimento de informações subjetivas filtradas pelos mecanismos de processamento de dados pessoais que, por sua vez, moldam a realidade para cada um apresentado. É a modulação comportamental subjetiva pelo exercício coletivo de poder nas redes virtuais:

> O cordão umbilical digital que liga as partes em uma relação imaterial é explorado para atualizar os serviços e produtos fornecidos com saída frequente e é customizado graças à aquisição e conhecimento de dados. Essa personalização vai além do indivíduo, colocando novas questões para a disponibilidade de dados como ativo competitivo (QUINTARELLI, 2019, p. 4).

A autoridade é estabelecida pela técnica, o que configura uma nova dimensão material do poder, "em que sistemas impessoais de disciplina e controle produzem certo conhecimento do comportamento humano independentemente do consentimento" (ZUBOFF, 2018, p. 42). Trata-se de uma nova arquitetura universal – chamada *Big Other*. Essa nova arquitetura reconfigura a estrutura de poder, que não mais se resume ao exercício totalitário e centralizado, conforme o modelo de Bentham, redesenhado na sociedade disciplinar por Foucault (1999). É um poder descentralizado, contínuo e sem rotas de fuga, em conformidade com interesses financeiros e ideológicos que invadem a vida privada.

A publicidade desempenha um papel essencial no capitalismo ao promover o incentivo ao consumo por meio da imposição de estilos de vida. O acesso, o tratamento e a disposição de dados pessoais exacerbaram a função da publicidade que, recorrendo a testes estatísticos, identifica as estratégias que mais influem no comportamento de cada consumidor especificamente.

O mundo da propaganda e do *marketing* resume-se a contar a história e a mensagem certa. O *Big Data* reúne uma crescente produção de dados em um suporte digital,

[11] Para Enriquez (2004, p. 49, tradução nossa), "desde que não nos esqueçamos de que o que antes era invisível à cota de intimidade, a vida interior de cada um, agora deve ser obrigatoriamente exposto no público (sobretudo nas telas de TV, mas também no palco literário), devemos entender que aqueles que prezam sua invisibilidade tendem a ser rejeitados, postos de lado ou transformados em suspeitos de um crime. A nudez física, social e psicológica está na ordem do dia".

caracterizando-se pelo volume, pela velocidade, pela variedade, pelo valor e pela veracidade[12]. Possibilita a modulação de dados e o direcionamento publicitário ao público-alvo específico, o que enseja o sucesso da mensagem, gera redução dos custos e aumento dos lucros pela provável venda do produto indicado (AKERLOF; SHILLER, 2016).

Como exemplo, pode-se citar a empresa Target. Há aproximadamente 18 anos, ela modificou o perfil da publicidade para torná-la mais subjetiva. Por isso, a empresa buscou analistas de números para formar programas para armazenar e cruzar os dados dos consumidores, a fim de atribuir-lhes um código de identificação, para garantir a publicidade personalizada, por meio de envios de cupons e de anúncios direcionados, conforme as suas necessidades, gostos e preferências. A Target conseguia identificar as futuras mamães pela previsibilidade nas compras, como grandes quantidades de loção sem perfume, estoque de vitaminas, desinfetantes para mãos, grande quantidade de toalhas de mãos etc. Eram mais de 25 itens específicos para categorizar essas consumidoras e, assim, enviar-lhes catálogos específicos com promoções e indicações de produtos e serviços[13]. No mesmo sentido, McDonald's, CBS, Mazda e Microsoft monitoravam e traçavam perfis de hábitos para direcionar a publicidade, tendo sido, em 2011, processadas pelo estado de Nova Iorque pela invasão de privacidade (DUHIGG, 2012).

Assim, a revolução tecnológica trouxe a redução das incertezas mercadológicas ao criar, por meio do *Big Data*, bolhas de filtros das predileções dos consumidores. É difícil definir o valor de tais informações, essenciais para operar mercados individualizados, as quais são facilmente captadas do cidadão-consumidor que utiliza a *web*. Com efeito, o rastreamento comportamental permite a programação de sofisticadas técnicas de publicidade.

Ressalta-se que dado e informação não são sinônimos, apesar de serem utilizados como se fossem. Os dados são conhecimentos brutos que podem ser refinados e revertidos em

---

[12] *Big Data* – termo mais generalizado e abrangente – caracteriza-se pelo volume de dados disponíveis, pela velocidade em que esses dados são produzidos, pelas fontes de coleta, pela correspondência com a informação atualizada e pela definição da abordagem que será feita da massa coletada (MITSUICHI, 2020). Para Zuboff (2018), o *Big Data* não pode ser entendido apenas como uma técnica de processamento de dados, trata-se de um conceito generalista e aberto que precisa considerar, inclusive, implicâncias sociais.

[13] Na Target, o seu analista de dados criou um modelo de previsão de gravidez e, com base nesse sistema, enviavam um catálogo específico com cupons para parabenizar a futura mãe. Um senhor, após receber tais anúncios e cupons para roupas de bebês e berço em casa, foi diretamente à loja da Target em Minnesota para reclamar, destacando que aquele ato poderia ser interpretado como um incentivo a sua filha, menor de idade, para que engravidasse. Dias depois, o gerente ligou ao cliente para pedir desculpas e recebeu a seguinte informação: "Tive uma conversa com minha filha, ele disse. Pelo jeito, estão acontecendo coisas nesta casa das quais eu não estava totalmente ciente. Ele respirou fundo. Ela vai ter o filho em agosto. Eu lhe devo um pedido de desculpas" (DUHIGG, 2012, p. 209).

informações objetivas, por meio do *Business Intelligence*[14]. Podem referir-se a uma pessoa identificada ou abstrata, por isso, é possível falar em dados pessoais e em dados (pseudo)anonimizados[15], respectivamente. Dão origem a um sistema informativo que possibilita conhecer e prever comportamentos, abrindo caminho para o "uso generalizado de técnicas psicométricas que permitem oferecer às pessoas produtos e serviços especificamente voltados a elas no momento em que os algoritmos detectam que elas estão mais propensas a adquirir o que lhes é oferecido" (ABRAMOVAY; ZANATTA, 2019, p. 161).

O poder, portanto, opera com base em valores, de forma contínua, em diferentes níveis, valendo-se o tempo todo de informações individuais obtidas em redes coletivas. Segue a lógica do conhecimento, do controle e da vigilância, intervindo por meio de sugestões e de direcionamento comportamental, como, por exemplo, por meio da publicidade. Estar-se-ia, então, diante de um novo modelo de governabilidade neoliberal cujo mecanismo de produção de subjetividade está centrado na economia de dados? Cabe o questionamento.

2.1 Os dados dos consumidores como um ativo na economia: formas de coleta, tratamento e circulação

Como se viu, diante da constante necessidade de personalização dos bens e serviços em busca da fidelização de clientes e da criação de nichos mercadológicos, o *marketing* desvinculou-se de ofertas e publicidades de massa, optando pelas individualizadas, singularizadas e altamente qualificadas. Assim, os dados pessoais tornaram-se o maior ativo da

[14] O *Business Intelligence* é complementar ao *Big Data*, sendo uma ferramenta mais objetiva para auxiliar a coleta, a condensação, o monitoramento, a filtragem e a organização de informações para a tomada de decisões estratégicas (QUAL..., 2020).

[15] Dados anonimizados não apresentam qualquer identificação subjetiva. No entanto, a doutrina discute a necessidade de os controladores e operadores de dados informarem todo o processo de anonimização e seus riscos para a análise da possibilidade de instauração da engenharia reversa com base em critérios objetivos e subjetivos e, consequentemente, para a reidentificação do sujeito (BIONI, 2020b). Tal discussão foi ampliada com a utilização de dados anonimizados por empresas de telefonia, solicitada pelos governos estaduais, para análise de fluxo durante a pandemia da Covid-19, principalmente no que diz respeito à reversão de informações anonimizadas e a seu tratamento pós-pandemia. Em 25 de abril de 2020, a Ministra Rosa Weber, concedeu liminar, por meio da ADI n.º 6390, para suspender a MP n.º 954/2020, cujo teor permitia que empresas de telefonia repassassem dados de clientes, pessoas físicas e jurídicas, como nome, endereço e telefone, ao IBGE. Tal liminar foi confirmada pelo STF em 6 e 7 de maio. No entanto, no que diz respeito à transparência do processo de anonimização para análise de movimentação por meio dos dados, não há ainda nenhuma decisão.

economia atual por possibilitarem a criação de estratégias mercadológicas “customizadas”, o que garante lucratividade e estabilidade[16].

Com tecnologia específica, as empresas conhecem o consumidor, seus gostos, predileções e interesses. No entanto, o consumidor tem um restrito acesso às informações mercadológicas do fornecedor. Existe uma concreta assimetria entre as informações na relação, uma vez que o consumidor está extremamente exposto ao processo de coleta e de tratamento de dados. Por isso, fala-se em “consumidor de vidro”:

> Somos todos consumidores de vidro, os outros sabem tanto sobre nós que quase conseguem ver através de nós. Nossas vidas cotidianas são registradas, analisadas e monitoradas de inúmeras maneiras, mas na maioria das vezes não percebemos, ou não pensamos nisso. Quando estamos cientes, podemos até aceitar – CCTV pode fazer-nos sentir mais seguros, podemos apreciar descontos recebidos como portadores de cartões de fidelidade de supermercados (LACE, 2005, p. 1, tradução nossa)[17].

O processo de tratamento de dados é dinâmico, é realizado por meio de operações técnicas, para simplificar e direcionar as informações. Comporta diversas atividades, mas, segundo Mendes (2019), o procedimento passa por três momentos: coleta, processamento e difusão de dados.

A coleta de dados pode ser feita com o conhecimento do consumidor ou secretamente. Pode ser consentida e informada ou com ausência de autorização. Pode ser colhida diretamente pelo fornecedor, pelo Estado ou por terceiros. A mais comum é feita por meio de transações comerciais, pesquisa de mercado e estilo de vida, sorteios e concursos, comercialização, cessão de dados e técnicas de controle por via da internet (MENDES, 2019).

A coleta de informações por via de transações comerciais tem por objetivo a fidelização do consumidor. Para que as informações sejam consideradas legítimas, devem ser obtidas por meio do consentimento. O armazenamento, o monitoramento e a classificação levam à análise do perfil de consumo de cada cliente.

As pesquisas de mercado reúnem informações disponibilizadas diretamente pelos consumidores. Servem para definir desejos e valor de mercado com o intuito de obter vantagem econômica. Já nos sorteios e concursos, os dados são coletados indiretamente, normalmente

---

[16] Para O’Neil (2020, p. 120), “a internet oferece aos anunciantes o maior laboratório que já existiu para pesquisa de consumidor e geração de leads. O feedback de cada divulgação chega em segundos – muito mais rápido que pelo correio. Em horas (ao invés de meses), cada campanha pode focar-se nas mensagens mais eficientes e chegar mais próxima de alcançar a brilhante promessa de toda publicidade: alcançar o interessado na hora certa, e com precisamente a melhor mensagem que provoque uma decisão, conseguindo assim mais um cliente pagador. Esse ajuste fino nunca cessa”.

[17] No original: “We are all ‘glass consumers’: others know so much about us, they can almost see through us. Our everyday lives are recorded, analysed and monitored in innumerable ways but mostly we do not realise, or think nothing of it. When we are aware, we may even welcome it — CCTV may make us feel safer, we may appreciate discounts received as supermarket loyalty cardholders”.

sem a indicação da finalidade de mercado pelos fornecedores. Os dados obtidos nos censos e nos registros públicos são considerados manifestamente públicos e são usados pelos fornecedores para mapear e classificar o consumidor.

Destacam-se ainda as tecnologias de controle como mecanismo de armazenamento de dados. Para Castells (2015, p. 176-177), tais tecnologias podem ser divididas de acordo com sua finalidade – identificação, vigilância e investigação:

> As tecnologias de identificação incluem o uso de senhas, "cookies" e procedimento de autenticação [...]. Baseiam-se frequentemente em tecnologia de criptografia. A autenticação opera muitas vezes em camadas, com usuários individuais sendo identificados por servidores que são eles próprios identificados por redes. [...]
> As tecnologias de vigilância são de um tipo diferente, mas muitas vezes se baseiam em tecnologias de identificação para localizar o usuário individual. As tecnologias de vigilância interceptam mensagens, instalam marcadores que permitem o rastreamento de fluxos de comunicação a partir de uma localização específica de computador e monitoram a atividade de máquinas 24 horas por dia. Tecnologias de vigilância podem identificar um dado servidor na origem de uma mensagem. [...]
> As tecnologias de investigação referem-se à construção de bancos de dados a partir dos resultados da vigilância e do armazenamento de informação rotineiramente registrada (Garfinkel, 2000). Uma vez que dados são coletados em forma digital, todos os itens de informação contidos no banco de dados podem ser agregados, desagregados, combinados e identificados de acordo com o objetivo e o poder legal. Por vezes, trata-se simplesmente de fazer perfis agregados, como em pesquisa de mercado, seja para o comércio ou para a política. Em outros casos trata-se de visar indivíduos, já que uma dada pessoa pode ser caracterizada por um grande corpo de informação contido em seus registros eletrônicos, de pagamentos por cartão de crédito a visitas a websites, correio eletrônico e chamadas telefônicas.

Os *cookies* são exemplos de tecnologia de controle de dados usada para identificação. Permite a memorização, a personalização do serviço e, se utilizada por um longo período, o rastreamento do comportamento do usuário (MENDES, 2019). Para Sánchez-Ocaña (2013), os *cookies* são pequenos fragmentos de informação que guardam dados de navegação ou informações sobre preferências. Ficam armazenados na rede e podem ser recuperados pelo servidor em futuras visitas.

Em outro sentido, o *spyware* é um programa classificado como uma tecnologia de vigilância. Por meio da intercepção de mensagens, do rastreamento do fluxo de comunicação e do monitoramento ininterrupto das atividades da máquina, monitora e remete informações a terceiros (MENDES, 2019).

Já as técnicas de processamento de dados, como tecnologia de investigação, têm como finalidade o refinamento de informações coletadas para alimentar novos processos, decisões e estratégias, em grande parte para práticas mercadológicas. Podem-se citar como exemplos de tais técnicas: *data warehousing* (DW), *online analytical processing* (OLAP), *data mining*, construção de perfil ou *profiling* e o *scoring*.

Data warehousing permite o gerenciamento dos dados para classificação dos usuários. Trata-se de um "depósito de dados, é um sistema informatizado que armazena enorme quantidade de informações e está organizado de tal modo a facilitar a extração de relatórios, o exame de grande volume de dados, bem como a tomada de decisão" (MENDES, 2019, p. 108). É uma forma de administração de informações diante do armazenamento de um grande volume de dados, uma vez que a correta manipulação poderá dinamizar setores da organização e fornecer indicadores de maneira integrada que auxiliam a gestão estratégica das corporações:

> DW é uma forma de gerir volumes muito grande de dados que se encontram, geralmente, espalhados em diversos sistemas de uma organização. Ele possibilita a análise de grandes volumes de dados coletados dos sistemas transacionais (OLTP). Em outras palavras, os DW das corporações são construídos a partir dos diferentes bancos de dados gerenciais de uma organização. (RASLAN; CALAZANS, 2014, p. 31).

Nesse sentido, o *data warehousing* estabelece uma estrutura que possibilita a identificação de tendências e de curvas de comportamentos e, consequentemente, auxilia no posicionamento estratégico das empresas. Não pode ser entendido como um *software*, mas é um sistema que "deve ser pensado como um processo que está sempre em crescimento para disponibilizar informações que apoiem as decisões estratégicas da organização" (RASLAN; CALAZANS, 2014. p. 32), sendo o núcleo dos sistemas de informações gerenciais e o apoio para as principais decisões de inteligência de mercado (ABDALLA; GUESSE, 2012).

O DW pode ser feito por inúmeras técnicas, como o OLAP, a construção de perfis e o *data mining* (MENDES, 2019). A exploração mais popular é realizada pelo OLAP ou processamento analítico em tempo real. É similar à técnica do *data mining*, divergindo na ferramenta de exploração: o DW é feito com base na verificação, ou seja, apenas confirma a hipótese elaborada, enquanto o *data mining* busca informações parcialmente ou totalmente desconhecidas pelos analistas de dados.

Assim, o *data mining* ou mineração de dados é o processo usado para encontrar padrões e transformar os dados complexos, de difícil compreensão, em informações, por meio de técnicas informáticas e estatísticas. Geralmente busca classificar pessoas ou objetos (MENDES, 2019), o que possibilita a caracterização do perfil comportamental do consumidor para ajudar na tomada de decisões estratégicas.

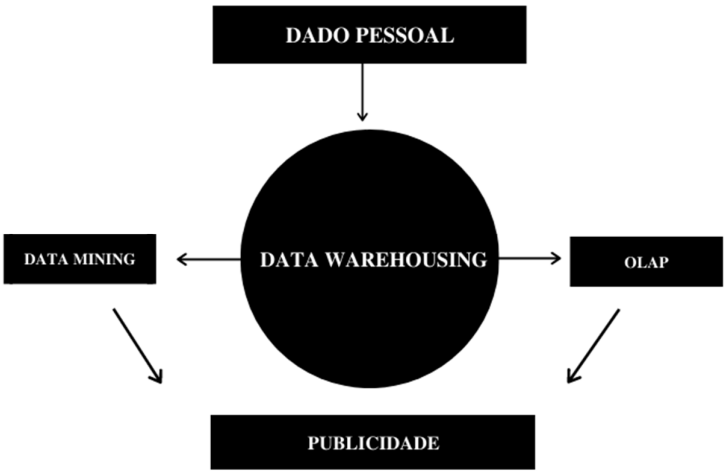
Como exemplo de técnica da mineração de dados, pode-se citar a identificação do perfil do cliente para publicidade direcionada para redes de *fast-food* (TAMA, 2015). Os dados do cliente são analisados, usando-se o método de mineração de dados com técnicas de classificação para indicar o produto ou serviço que melhor se enquadra no perfil:

> [O] período de captação foi definido de forma a refletir o comportamento de vendas da loja em dias normais de operação. A base de dados foi preparada (i.e., pré-

> processada) e submetida ao processo de mineração de dados em busca de associações entre produtos que fossem vendidos de forma conjunta e frequente pela loja (tarefa de Descoberta de Associações). Algumas associações entre produtos foram consideradas interessantes e promoções para estimular a venda combinada de tais produtos foram realizadas com êxito (GOLDSCHMIDT; BEZERRA, 2016).

É importante destacar que tal procedimento poderá identificar dados sensíveis, que se afastam da finalidade exposta pela empresa ao consumidor. Por isso, apenas será legítimo com o prévio consentimento expresso do consumidor (MENDES, 2019). A Figura 1 mostra o esquema do tratamento de dados por meio de DW, OLAP ou *data mining*.

Figura 1 – *Business Inteligence* por meio de DW.



Fonte: Elaboração da autora.

A construção de perfil ou *profiling* faz uma junção de dados "com finalidade de se obter uma imagem detalhada e confiável, visando, geralmente, à previsibilidade de comportamentos, de gostos, hábitos de consumo e preferencias do consumidor" (MENDES, 2019, p. 111).

De acordo com um relatório elaborado pelo Bureau of Consumer Protection[18] do Federal Trade Commission (2000), a realização do *online profiling* tem por base a utilização de *cookies* que, por meio de um fluxo de *clicks* e da combinação de informações, consegue identificar e criar o perfil do consumidor. Tal estudo ressaltou ainda que, para a criação do perfil, há o

[18] "The profiles created by the advertising networks can be extremely detailed. A cookie placed by a network advertising company can track a consumer on any Web site served by that company, thereby allowing data collection across disparate and unrelated sites on the Web. Also, because the cookies used by ad networks are generally persistent, their tracking occurs over an extended period of time, resuming each time the individual logs on to the Internet. When this 'clickstream' information is combined with third-party data, these profiles can include hundreds of distinct data fields" (FEDERAL TRADE COMMISSION, 2000, p. 5-6).

cruzamento de informações não identificáveis e identificáveis do consumidor. Daí o questionamento sobre a real possibilidade de anonimização dos dados pessoais.

O objetivo de tais técnicas de coleta e de tratamento é entender o perfil de cada consumidor para direcionar a publicidade conforme seus gostos e interesses e impulsionar as vendas. Trata-se, portanto, de uma atividade pré-contratual, por vezes desconhecida pelo próprio consumidor, a qual possibilita maior êxito na realização do negócio jurídico e transforma o consumidor ao mesmo tempo em destinatário final e matéria-prima da relação consumerista virtual.

2.2 O novo modelo de negócio *on-line*: o *microtargeting*

Microtargeting – microssegmentação – é um processo de amostragem baseado na segmentação detalhada do público-alvo para criação de mensagens e ofertas personalizadas, principalmente para a realização de comerciais *on-line*, mas também para campanhas eleitorais.

Han (2018) destaca que o *microtargeting* é uma estratégia bastante utilizada em eleições para abordar eleitores por meio de mensagens direcionadas e personalizadas. Os algoritmos são excelentes para aperfeiçoar discursos ao individualizá-los, tendo mais força para influenciar o comportamento de cada um. Nesse sentido, "votar e comprar, Estado e mercado, cidadão e consumidor se assemelham" (HAN, 2018, p. 87):

> Nos EUA, várias empresas oferecem serviços de microtargeting *on-line*, especialmente a políticos. Por exemplo, empresas como CampaignGrid e Cambridge Analytica permitem que os políticos atinjam pessoas com anúncios no Facebook, LinkedIn e outros *sites* da Web. A Cambridge Analytica afirma ter coletado "até 5.000 dados de 230 milhões de eleitores americanos". A empresa tenta identificar as características da personalidade das pessoas para prever que tipo de mensagem tem mais probabilidade de convencer as pessoas (BORGESIUS *et al.*, 2018, p. 83, tradução nossa)[19].

No mercado, tal processo já é utilizado há aproximadamente vinte anos. Primeiramente, os códigos postais eram usados para fazer uma segmentação geográfica e, assim, personalizar a oferta e a publicidade conforme a região. Posteriormente, as técnicas relacionadas com *microtargeting* evoluíram na identificação e na análise de informações obtidas de perfis pessoais dos usuários de internet, especialmente das redes sociais.

Para ser considerada eficiente, a *microtargeting* deve respeitar algumas etapas:

> Em primeiro lugar, as necessidades do público-alvo devem ser determinadas com precisão. Isso é feito por meio do estudo do segmento pretendido do mercado,

[19] No original: "In the US, several companies offer online microtargeting services especially to politicians. For instance, companies like CampaignGrid and Cambridge Analytica enable politicians to target people with ads on Facebook, LinkedIn, and elsewhere on the web. Cambridge Analytica claims to have collected 'up to 5,000 data points on over 230 million American voters'. The company attempts to identify people's personality traits to predict what kind of message is most likely to persuade people".

> incluindo o comportamento do usuário como resulta do uso de redes de mídia social e do comportamento do consumidor em relação a produtos similares. O segundo passo é projetar um produto para atender a essas necessidades da melhor maneira possível, com o discurso, a abordagem e a resposta apropriados às necessidades mencionadas. O terceiro passo é apresentar o produto ao público-alvo e direcionar um diálogo microssegmentado, bem como avaliar os resultados (BARBU, 2014, p. 47, tradução nossa)[20].

Assim, para realizar a microssegmentação dos consumidores, ferramentas como *geoblocking* e *geopricing* são utilizadas com a finalidade de individualizar e, consequentemente, de especificar a oferta e a publicidade, conforme se verá a seguir.

2.2.1 *Geoblocking* e *geopricing* como ferramentas de *microtargeting*

No que diz respeito à segmentação do consumidor, as práticas de *microtargeting* podem realizar distinções geográficas, destacando-se, especialmente, as ferramentas chamadas *geoblocking* e *geopricing*.

Para Morassutti (2019), o protocolo chamado *Transmission Control Protocol/Internet Protocol* (TCP/IP) permite a identificação do controle, a verificação das transmissões de mensagens enviadas e seu endereçamento lógico, ou seja, a indicação da máquina, sua localização e sua conexão. As práticas de *geoblocking* e *geopricing* seguem essa estratégia.

Geoblocking é uma ferramenta pela qual um fornecedor limita o acesso de certos consumidores a seus bens e serviços com base em sua localização ou nacionalidade. Para Morassutti (2019), não há um consenso sobre a sua definição, no entanto, pode-se afirmar que o *geoblocking* é "qualquer técnica de restrição ou discriminação de fluxo de dados baseada em algum indicador de geolocalização do usuário da rede, tais como cruzamento do endereço IP e uma base de dados de geolocalização" (MORASSUTTI, 2019, p. 3).

O Regulamento Europeu 2018/302 (UNIÃO EUROPEIA, 2018) proíbe as práticas injustificadas de *geoblocking*, definindo o termo como uma prática discriminatória pelo bloqueio ou pela limitação do acesso em razão do território ou da nacionalidade do consumidor. Conforme Mendieta (2019), esse regulamento visa evitar a discriminação nas transações

[20] No original: "Firstly, the needs of the target audience have to be accurately determined. This is done by studying the intended segment of the market, including user behavior as results from social media networking usage and consumer behaviorism in relation to similar products. The second step is designing a product to cover these needs as best as possible, one with the appropriate discourse, approach and response to the said needs. The third step is made out of presenting the product to the target audience and directing a microtargeted dialogue as well as evaluating the results".

transfronteiriças com base na nacionalidade, no local de residência ou na localização física dos clientes[21].

Ressalta-se que tal regulamento proíbe quaisquer tipos de bloqueio, limitação e redimensionamento do consumidor para uma interface diferente daquela em que pretendia realizar a relação comercial[22], bem como impede a limitação no que diz respeito ao pagamento do produto e/ou serviço para evitar qualquer prática considerada discriminatória por causa da territorialidade ou da nacionalidade[23]. O objetivo do Regulamento é evitar uma distinção injustificada com base na territorialidade (MENDIETA, 2019).

Quanto à prática de *geopricing*, trata-se da utilização da geolocalização como critério para diferenciação de preço entre os consumidores. Tanto a *geoblocking* quanto a *geopricing* podem ser consideradas como discriminatórias e atentatórias aos princípios consumeristas, especialmente de acordo com os artigos 6.º, II, e 39, II e IX, do CDC, com o artigo 36, parágrafo 3, X, da Lei n.º 12.529/2011 e o artigo 9.º da Lei n.º 12.965/2014 – Marco Civil da Internet. Para Morassutti (2019, p. 7), essas ferramentas são prejudiciais ao consumidor pelas seguintes razões:

> a) recusar atendimento de consumidores; b) recusar venda de produtos ou serviços a quem se disponha a fazê-lo mediante pronto pagamento, ressalvadas as hipóteses previstas em leis especiais; c) fixar de modo diferenciado preços ou outras condições no fornecimento de produtos ou serviços, quando a diferenciação puder produzir prejuízo à livre-concorrência, domínio de mercado relevante, aumento arbitrário dos lucros ou exercício abusivo de posição dominante; d) tratar não isonomicamente, durante a transmissão, comutação ou roteamento, de quaisquer pacotes de dados, ressalvadas as hipóteses previstas em lei.

---

[21] Artigo 1.º: "1. O presente regulamento tem por objetivo contribuir para o correto funcionamento do mercado interno, evitando o bloqueio geográfico injustificado e outras formas de discriminação baseadas, direta ou indiretamente, na nacionalidade, no local de residência ou no local de estabelecimento dos clientes, nomeadamente tornando mais claras certas situações em que uma diferença de tratamento não pode ser justificada ao abrigo do artigo 20.º, n.º 2, da Diretiva 2006/123/CE" (UNIÃO EUROPEIA, 2018, p. 9).

[22] Artigo 3.º: "1. Os comerciantes não podem bloquear nem restringir, por meio de medidas de caráter tecnológico ou de qualquer outro modo, o acesso dos clientes às suas interfaces em linha por razões relacionadas com a nacionalidade, com o local de residência ou com o local de estabelecimento dos clientes. 2. Os comerciantes não podem redirecionar os clientes, por razões relacionadas com a nacionalidade, com o local de residência ou com o local de estabelecimento do cliente, para uma versão da sua interface em linha diferente da interface em linha a que o cliente tentou aceder inicialmente, em virtude da sua configuração, da utilização de um idioma ou de outros fatores que deem a essa interface em linha características específicas para clientes com uma nacionalidade, um local de residência ou um local de estabelecimento determinados, a não ser que o consumidor tenha dado o seu consentimento expresso para esse redirecionamento" (UNIÃO EUROPEIA, 2018, p. 11).

[23] Artigo 5.º: "1. Os comerciantes não podem aplicar, no âmbito dos instrumentos de pagamento por si aceites, por razões relacionadas com a nacionalidade, com o local de residência ou com o local de estabelecimento do cliente, com a localização da conta de pagamento, com o local de estabelecimento do prestador de serviços de pagamento ou com o local de emissão do instrumento de pagamento na União, diferentes condições a operações de pagamento, caso: a) As operações de pagamento sejam efetuadas através de uma transação eletrónica mediante transferência bancária, através de débito direto ou através de um instrumento de pagamento baseado em cartões da mesma marca e da mesma categoria; b) Os requisitos de autenticação sejam cumpridos nos termos da Diretiva (UE) 2015/2366; e c) As operações de pagamento sejam efetuadas numa moeda aceite pelo comerciante" (UNIÃO EUROPEIA, 2018, p. 12).

Como exemplo, destaca-se a ação civil pública[24] movida pelo Ministério Público do Estado do Rio de Janeiro contra Decolar.com LTDA., fundamentada na instauração do Inquérito Civil n.º 347/PJDC/2016, que verificou a ocorrência de transgressão coletiva da empresa de comércio eletrônico pela realização de *geopricing* e *geoblocking*. A empresa estaria utilizando os dados pessoais dos consumidores, com base em suas informações sobre a origem geográfica e nacionalidade, para bloquear ofertas e atribuir preços mais altos.

Apesar de serem consideradas práticas controversas, a *geoblocking* e a *geopricing* são extremamente utilizadas para direcionamento de oferta e publicidade. Como visto na subseção 2.2, a publicidade direcionada é a última etapa do processo de *microtargeting*. Por meio dela, haverá a comunicação individualizada entre o fornecedor e o consumidor com prováveis chances de êxito diante da sua formulação conforme predileções de cada um. Trata-se de uma tentativa de manipulação do consumidor de vidro, exposto e influenciado, de acordo com os interesses do mercado.

2.3 A publicidade como veículo pré-contratual e sua nova dimensão no ambiente virtual

Segundo o artigo 8.º da Seção 2.ª do capítulo 1.º do Código Brasileiro de Autorregulamentação Publicitária, a publicidade e a propaganda são "atividades destinadas a estimular o consumo de bens e serviços, bem como promover instituições, conceitos ou ideias". Existe uma distinção doutrinária entre tais termos: a publicidade é direcionada à atividade comercial, enquanto a propaganda possui um caráter ideológico, diverso do mercadológico, e não visa, a princípio, a lucratividade do anunciante.

Para Freitas (1998), a publicidade tem a finalidade de englobar informações e ações do fornecedor para estimular o consumo de produtos ou serviços, além de promover a atividade econômica. Define-se como "toda e qualquer ação do fornecedor, destinada ao consumidor, com o fim de estimular a aquisição ou utilização de produtos ou serviços, visando promover uma determinada atividade econômica" (FREITAS, 1998, p. 3). No mesmo sentido, Rodrigues (2019, p. 117) destaca:

> A publicidade é uma prática mercadológica que não apenas informa o consumidor acerca da existência de produtos e serviços como, mais que isso, tem o poder de despertar o seu interesse e desejo de compra. Trata-se de prática inerente ao próprio funcionamento do mercado de consumo, que encontra respaldo constitucional tanto na perspectiva econômica, enquanto desdobramento da livre iniciativa e da livre concorrência, como, também, sob a ótica do princípio da liberdade de expressão.

[24] Tribunal de Justiça do Estado do Rio de Janeiro (Vigésima Sétima Câmara Cível). Ação Civil Pública. Processo n.º 0018051-27.2018.8.19.0001. Agravante: Ministério Público do Rio de Janeiro. Agravado: Decolar.com. Publicação em 6 fev. 2018.

Nesse sentido, a função da publicidade está diretamente relacionada com a capacidade de influenciar o comportamento do consumidor e de possibilitar o conhecimento do serviço ou produto com o fito de motivar o ato de consumo (RODRIGUES, 2019). Na mesma perspectiva, Lopes (2011) aduz que à publicidade cabe informar para destacar as qualidades do produto ou do serviço com a intenção de persuadir a prática do consumo. A publicidade institucional busca promover a imagem do fornecedor, e a promocional atrela-se à venda de um produto específico.

Os limites da publicidade estão dispostos no CDC (Lei n.º 8.078/1990), nos seus artigos 6.º, inciso IV[25], e 30 a 38[26]. A publicidade integra a oferta, que é feita com base em informações ou pela publicidade em si, tendo por base o princípio da transparência e o dever de informação, uma vez que devem ser asseguradas "informações corretas, claras, precisas, ostensivas, em língua portuguesa sobre características, qualidade, quantidade, composição, preço, garantia de prazos de validade e origem", conforme artigo 31 do CDC.

[25] "Art. 6º São direitos básicos do consumidor: [...] IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços".

[26] "Art. 30. Toda informação ou publicidade, suficientemente precisa, veiculada por qualquer forma ou meio de comunicação com relação a produtos e serviços oferecidos ou apresentados, obriga o fornecedor que a fizer veicular ou dela se utilizar e integra o contrato que vier a ser celebrado. Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores. Parágrafo único. As informações de que trata este artigo, nos produtos refrigerados oferecidos ao consumidor, serão gravadas de forma indelével. (Incluído pela Lei n.º 11.989, de 2009). Art. 32. Os fabricantes e importadores deverão assegurar a oferta de componentes e peças de reposição enquanto não cessar a fabricação ou importação do produto. Parágrafo único. Cessadas a produção ou importação, a oferta deverá ser mantida por período razoável de tempo, na forma da lei. Art. 33. Em caso de oferta ou venda por telefone ou reembolso postal, deve constar o nome do fabricante e endereço na embalagem, publicidade e em todos os impressos utilizados na transação comercial. Parágrafo único. É proibida a publicidade de bens e serviços por telefone, quando a chamada for onerosa ao consumidor que a origina. (Incluído pela Lei n.º 11.800, de 2008). Art. 34. O fornecedor do produto ou serviço é solidariamente responsável pelos atos de seus prepostos ou representantes autônomos. Art. 35. Se o fornecedor de produtos ou serviços recusar cumprimento à oferta, apresentação ou publicidade, o consumidor poderá, alternativamente e à sua livre escolha: I - exigir o cumprimento forçado da obrigação, nos termos da oferta, apresentação ou publicidade; II - aceitar outro produto ou prestação de serviço equivalente; III - rescindir o contrato, com direito à restituição de quantia eventualmente antecipada, monetariamente atualizada, e a perdas e danos. Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal. Parágrafo único. O fornecedor, na publicidade de seus produtos ou serviços, manterá, em seu poder, para informação dos legítimos interessados, os dados fáticos, técnicos e científicos que dão sustentação à mensagem. Art. 37. É proibida toda publicidade enganosa ou abusiva. § 1.º É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falso, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços. § 2.º É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança. § 3.º Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço. § 4.º (Vetado). Art. 38. O ônus da prova da veracidade e correção da informação ou comunicação publicitária cabe a quem as patrocina".

No mesmo sentido, de acordo com o Código Brasileiro de Autorregulamentação Publicitária, a publicidade deve ter por base anúncios honestos e verdadeiros (arts. 23[27] e 27[28]) e deve velar pela intimidade, respeitando a dignidade da pessoa humana e da família (art. 34, alínea c[29]).

Tais informações estão incorporadas pré-contratualmente ao negócio a ser realizado e, consequentemente, vinculam o fornecedor. Em caso de impossibilidade ou recusa do fornecedor em cumprir a oferta, o artigo 35 do CDC dispõe que o consumidor poderá exigir o cumprimento forçado, aceitar outro produto ou prestação equivalente e, ainda, rescindir o contrato.

A publicidade deve ser veiculada de forma clara para que o consumidor a identifique de maneira imediata (art. 36 do CDC), com base em três princípios fundamentais: a) o princípio da identificação, b) o princípio da veracidade e c) o princípio da vinculação (MIRAGEM, 2016, p. 271).

No que diz respeito ao princípio da identificação, o consumidor deve facilmente entender que se trata de anúncios publicitários. Por isso, as publicidades subliminares e clandestinas são consideradas problemáticas: a ausência de transparência na sua circulação pode ofuscar a intenção econômica. A publicidade subliminar trabalha com estímulos sonoros e visuais não perceptíveis pelo consciente, que penetram o subconsciente por causa da repetição; já a publicidade clandestina omite o caráter publicitário da informação, como no caso do *merchandising*[30] ou do *product placement*[31].

O princípio da veracidade está diretamente relacionado com o estabelecimento da boa-fé objetiva nos contratos de consumo, devendo todos os atos ser realizados com lealdade e transparência. Portanto, toda informação deverá "guardar relação de conformidade com os fatos

---

[27] "Artigo 23 Os anúncios devem ser realizados de forma a não abusar da confiança do consumidor, não explorar sua falta de experiência ou de conhecimento e não se beneficiar de sua credulidade".

[28] "Artigo 27 O anúncio deve conter uma apresentação verdadeira do produto oferecido, conforme disposto nos artigos seguintes desta Seção, onde estão enumerados alguns aspectos que merecem especial atenção".

[29] "Artigo 34 Este Código condena a publicidade que: [...] c. revele desrespeito à dignidade da pessoa humana e à instituição da família".

[30] Explicita Lopes (2011, p. 5): "Referimos à prática de, sutilmente, sem alertar-se para o fato de tratar-se de mensagem publicitária, inserirem-se anúncios comerciais em meio a programas de televisão, cinema, etc. Aqui, como na concepção original do *merchandising*, o vendedor é silencioso, porque não confessa o fim publicitário da mensagem".

[31] Para Rodrigues (2019, p. 132), "o *product placement* ou colocação do produto consiste em uma estratégia que busca associar circunstâncias ou eventos cotidianos à adoção de um determinado estilo de vida, que, por sua vez, remete à aquisição de produtos ou serviços específicos. A intenção de quem veicula a publicidade é fazer com que o consumidor acredite que, caso queira usufruir daquele estilo de vida, deverá adquirir os bens de consumo a ele associados por meios de mensagem publicitária".

de natureza técnica ou científica relativos ao produto ou serviço anunciado" (MIRAGEM, 2016, p. 275).

Já o princípio da vinculação está relacionado com o cumprimento integral dos termos do anúncio, conforme as disposições do artigo 35 do CDC.

Para o artigo 37 do CDC, é publicidade ilícita aquela considerada enganosa ou abusiva. Em linhas gerais, a publicidade enganosa contraria o dever de veracidade e de clareza para induzir o consumidor ao erro. Já a publicidade abusiva viola valores e bens jurídicos relevantes socialmente, como, por exemplo, a proteção do meio ambiente e a proteção da incolumidade do consumidor, por induzir ao exercício de atividade perigosa à saúde ou à segurança:

> A abertura normativa no conceito de publicidade abusiva é intencional, de modo a abranger, em sua definição, toda e qualquer mensagem publicitária que leve o consumidor a adotar um comportamento prejudicial à sua saúde ou segurança ou que ofenda a ordem pública, no sentido mais amplo do termo, por atentar contra valores sociais considerados fundamentais [...]. Concede maior margem de interpretação para o julgador, que na verificação do potencial abusivo de uma mensagem publicitária deverá examinar as suas particularidades, levando em consideração cada caso concreto, sempre com vistas a proteger os interesses coletivos (RODRIGUES, 2019, p. 140-141).

A realização da atividade publicitária tradicional envolve três agentes: o fornecedor de bens e/ou serviços, a agência de publicidade e o meio de comunicação, em atenção ao artigo 3.º do Código Brasileiro de Autorregulamentação Publicitária. No que diz respeito à responsabilização, há divergência doutrinária sobre o tema.

Para Grinover *et al*. (1999), a agência de publicidade só será responsável se concorrer dolosamente ou culposamente para o dado causado pela publicidade. Para Nunes (2017, p. 673), os agentes são solidariamente responsáveis pelos danos que os anúncios podem gerar "na medida de sua participação e/ou poder decisório". Para Verbicaro (2016), causa efeito pedagógico responsabilizar a agência por publicidade abusiva e enganosa, salvo quando o ilícito não está no anúncio em si ou quando depende de uma "ação real, ação concreta e posterior do fornecedor-anunciante, de maneira que a agência tenha participado como mera produtora de uma informação encomendada" (VERBICARO, 2016, p. 277).

Na mesma perspectiva, o Código de Autorregulamentação Publicitária, em seus artigos 45, alínea b[32], e 46[33], estabelece que os agentes são objetivamente e solidariamente responsáveis pelo planejamento, pela veiculação, pela criação e pela execução do anúncio.

A publicidade tradicional está diretamente relacionada com a tutela difusa, em razão da dimensão abstrata da exposição da coletividade. Assim, o CDC, no seu artigo 29[34], dispõe que o público-alvo publicitário é o grupo ao qual efetivamente a mensagem é direcionada, exposto, portanto, à publicidade. "Reconhecendo-se, portanto, a fragilidade inerente à coletividade, diante dos meios de convencimento em massa, das técnicas agressivas de captação de clientela, de que se utilizam os fornecedores, é que se justifica a tutela pré-contratual do consumidor" (VERBICARO, 2016, p. 268).

No entanto, é fato que a evolução tecnológica e a utilização de dados pessoais na prática do *microtargeting* modificaram diretamente o exercício da publicidade. Ela tem um caráter subjetivo e é realizada por agentes diversos da atividade tradicional, diante da necessidade da coleta, do processamento e da circulação dos dados. Trata-se, portanto, de uma publicidade direcionada, possível pela segmentação do consumidor de vidro, e, sem dúvida, um mecanismo eficaz para a persuasão ao consumo tendo em vista a lucratividade do fornecedor.

2.3.1 Publicidade direcionada: contextual, segmental e comportamental

A publicidade seguiu um caminho inverso da despersonificação e, consequentemente, da massificação das relações de consumo. O mercado entendeu que a comunicação em massa era custosa e, por vezes, ineficiente, por desperdiçar esforços em busca do público-alvo. Assim, com a evolução tecnológica, surgiu a publicidade direcionada para efetivar a comunicação com o consumidor e aumentar a propensão ao consumo: "a publicidade direcionada é uma prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo" (BIONI, 2020a, p. 15), podendo ser dividida em segmental, contextual e comportamental.

---

[32] "Artigo 45 A responsabilidade pela observância das normas de conduta estabelecidas neste Código cabe ao Anunciante e a sua Agência, bem como ao Veículo, ressalvadas no caso deste último as circunstâncias específicas que serão abordadas mais adiante, neste Artigo. [...] b. a Agência deve ter o máximo cuidado na elaboração do anúncio, de modo a habilitar o Cliente Anunciante a cumprir sua responsabilidade, com ele respondendo solidariamente pela obediência aos preceitos deste Código".

[33] "Artigo 46 Os diretores de qualquer pessoa empregada numa firma, companhia ou instituição que tomem parte no planejamento, criação, execução e veiculação de um anúncio, respondem, perante as normas deste Código, na medida de seus respectivos poderes decisórios".

[34] "Art. 29. Para os fins deste Capítulo e do seguinte, equiparam-se aos consumidores todas as pessoas determináveis ou não, expostas às práticas nele previstas".

A publicidade segmental visa um determinado público-alvo, independentemente do contexto da plataforma. Atende ao interesse de um grupo específico e adota uma linguagem adequada a esse segmento:

> veículo ou campanha publicitária dirigida a determinado público definido por critérios de sexo, idade, classe social ou uma combinação destes [...]. Uma mídia segmentada seria, assim, um veículo capaz de atingir com maior eficiência e economia esses públicos determinados ou uma campanha concebida e dirigida especialmente para esse público (FISHER, 2001, p. 3).

Como exemplo, pode-se citar o assédio discriminatório de gênero no mercado *on-line*. Determinadas campanhas são diretamente dirigidas ao público feminino, o que, por vezes, impõe padrões comportamentais e de consumo. O excessivo assédio de consumo a esse grupo individualizado faz com que as mulheres gastem mais com o consumo de bens e serviços específicos do que outras categorias (VERBICARO; ALCÂNTARA, 2017b).

A publicidade contextual está ligada a aspectos objetivos do ambiente veiculado. Leva, portanto, em consideração "o meio no qual é promovido o bem de consumo" (BIONI, 2020a, p. 15). Entende-se que, quando o consumidor acessa determinado *website*, ele tem interesse nos serviços e produtos vinculados a sua atividade.

A publicidade comportamental é a mais individualizada de todas. Utiliza aspectos subjetivos e personalizados do consumidor graças às ferramentas de coleta na *web* (subseção 2.1). Por meio da navegação, cria-se um retrato que possibilita precisar o perfil do consumidor, além de reduzir os custos e aumentar as chances de êxito do consumo:

> Quando o usuário navega na internet, há uma série de cliques (*clickstream*) que revela uma infinidade de informações sobre as suas predileções, possibilitando que a abordagem publicitária as utilize para estar precisamente harmonizada com elas. Desta forma, a publicidade online, pode ser direcionada com um grau de personalização jamais alcançado pela publicidade off-line (BIONI, 2020a, p. 17).

O Artigo 29[35] da Comissão Europeia faz uma distinção entre publicidade comportamental, segmental e contextual. Enquanto a primeira tem por base características do comportamento identificadas em ações *on-line*, como visitas repetidas a um *site*, interações, palavras-chave, conteúdo *on-line*, e visa a definição de um perfil específico, as duas últimas relacionam-se, respectivamente, com os sujeitos e suas ações em *sites* determinados. As três

[35] "Behavioural advertising is advertising that is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions (repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests. Whereas contextual advertising and segmented advertising use 'snap shots' of what data subjects view or do on a particular web site or known characteristics of the users, behavioural advertising potentially gives advertisers a very detailed picture of a data subject's online life, with many of the websites and specific pages they have viewed, how long they viewed certain articles or items, in which order, etc." (ARTICLE 29…, 2010, p. 4-5).

são tipos de publicidade direcionada, mas a primeira apresenta um nível maior de individualização.

A navegação em si na *web*[36], a utilização de redes sociais e de aplicativos de localização geográfica, como o GPS e o WAZE, ou de mensagens, inclusive a utilização de *emoticons*[37], possibilitam a publicidade direcionada. Facebook (FB)[38] e TweetFeel[39] (no Twitter), por exemplo, monitoram as conversas de sua rede para catalogar pensamentos, expressões e opiniões. O caso da empresa de análise de dados Cambridge Analytica[40] evidenciou a utilização de redes sociais, especialmente o Facebook, para a realização de *microtargeting* em campanhas eleitorais. No que diz respeito à publicidade direcionada, os próprios termos de privacidade da rede admitem a coleta de dados para esse fim[41].

2.3.2 Assédio de consumo *on-line* na publicidade direcionada

O assédio de consumo surge na sociedade para convencer o consumidor a adquirir um produto específico, por meio da publicidade direta, seja pela sugestão de envolvimento com o produto ou marca, seja pela difusão de risco de isolamento caso haja uma escolha diversa daquela que é sugerida:

> O assédio de consumo é caracterizado pela prática de condutas agressivas, que afetam diretamente a liberdade de escolha do consumidor, seus projetos de vida, atentando contra sua esfera psíquica, que, em meio de tantas estratégias manipuladoras, é subjugado e levado a ceder às pressões do mercado (VERBICARO; RODRIGUES; ATAÍDE, 2018, p. 169).

Nesse contexto, o assédio é visto, a princípio, não como uma agressão, mas como uma sensação de encantamento. Trata-se de um grande paradoxo, uma vez que o consumidor seduzido tem a sua liberdade de escolha diretamente violada e agredida (RODRIGUES, 2019):

---

[36] Para Sánchez-Ocaña (2013), os *cookies* do Google seguem-nos e monitoram-nos diariamente até sua data de vencimento – 2038, ou seja, compilam e armazenam dados pessoais, o que lhe permitirá ter um completo histórico de navegação *on-line*.

[37] Forma de comunicação paralinguística para expressar emoções nas redes.

[38] O Facebook já admitiu o monitoramento de postagens e de conversas dos usuários. A rede alegou que fiscaliza todas as conversas automaticamente para verificar se há violação dos termos de uso (GOGONI, 2018). Conforme Sánchez-Ocaña (2013, p. 141), "por meio dos cliques no botão curtir, o Facebook pode saber que tipos de filmes ou produtos eu prefiro. Esses dados são inacessíveis para o Google, o que afasta da posição que havia mantido até o momento e que lhe deu outrora a vantagem competitiva: ser aquele que melhor conhece os usuários e que, portanto, pode prever a sua conduta".

[39] O TweetFeel monitora conversas no Twitter, expressões negativas e positivas nessa rede.

[40] Ver o documentário *Privacidade Hakeada*, difundido em 2019 pela Netflix.

[41] Como exemplo, lê-se nos Termos de Privacidade de Utilização do Google, de 31 de março de 2020: "consoante as suas definições, também lhe podemos mostrar anúncios personalizados com base nos seus interesses. Por exemplo, se pesquisar 'bicicletas de montanha', pode ver um anúncio a equipamento desportivo quando estiver a navegar num site que mostre anúncios publicados pela Google" (TERMOS..., 2020).

> O assédio de consumo não busca excluir. Talvez por isso, possa ser percebido, também, nas práticas que aliciem ou que seduzam – *por meio da repetição* – o consumidor e, em especial, mas não exclusivamente, o idoso, o analfabeto, o doente e todo aquele que, por qualquer outra razão vivencie situação de vulnerabilidade extremada, buscando forçá-lo, constrangê-lo, aliciá-lo a adquirir produto, serviço ou obter acesso ao crédito (CATALAN; PITOL, 2017, p. 147, grifo dos autores).

Assim, o assédio trabalha com a compulsão irracional e com o consumismo. O consumidor tem a sua liberdade maculada pela forte pressão publicitária, no âmbito individual ou coletivo. O combate do assédio, portanto, está diretamente relacionado com a proteção do direito à liberdade de escolha, garantido, no Brasil, enquanto direito básico do consumidor, um direito que também consagra a proibição do recurso a métodos comerciais coercitivos e/ou desleais (CATALAN; PITOL, 2017).

Segundo o Anexo I da Directiva 2005/29/CE, são práticas comerciais agressivas, entre outras:

> 24. Criar a impressão de que o consumidor não poderá deixar o estabelecimento sem que antes tenha sido celebrado um contrato;
> 25. Contactar o consumidor através de visitas ao seu domicílio, ignorando o pedido daquele para que o profissional parta ou não volte, excepto em circunstâncias e na medida em que haja que fazer cumprir uma obrigação contratual, nos termos do direito nacional;
> 26. Fazer solicitações persistentes e não solicitadas, por telefone, fax, e-mail, ou qualquer outro meio de comunicação à distância excepto em circunstâncias e na medida em que haja que fazer cumprir uma obrigação contratual, nos termos do direito nacional. [...];
> 27. [...] deixar sistematicamente sem resposta a correspondência pertinente, com o objectivo de dissuadir o consumidor do exercício dos seus direitos contratuais;
> 28. Incluir num anúncio publicitário uma exortação directa às crianças no sentido de estas comprarem ou convencerem os pais ou outros adultos a comprar-lhes os produtos anunciados. [...] (UNIÃO EUROPEIA, 2005).

O CDC não indicou de forma explícita as práticas consideradas como assédio de consumo. No entanto, nos artigos 29, 37[42] e 39[43], destaca-se a proteção do consumidor quanto à oferta e à publicidade. De fato, em tais artigos, encontra-se um rol de práticas abusivas, tipos normativos abertos com indicações meramente exemplificativas, o que possibilita o seu enquadramento.

O excessivo direcionamento publicitário atinge a autonomia de vontade do consumidor, pois, além de estar diretamente associado ao ilegítimo exercício negocial do fornecedor, que

---

[42] Para Verbicaro, Rodrigues e Ataíde (2018, p. 172), "nessa mesma lógica, o CDC, entre os artigos 29 e 37, disciplina o consumidor exposto a práticas empresariais abusivas no âmbito pré-contratual, quando o induzem ao erro, maculando o seu direito de opção acerca do produto ou serviço, criando, inclusive, obstáculos à compreensão do alcance do contrato".

[43] Para Rodrigues (2019, p. 39), "o artigo 39 do Código de Defesa do Consumidor apresenta um rol meramente exemplificativo de práticas abusivas, e se o assédio de consumo é uma prática violadora de direitos do consumidor, pode-se dizer que pelo arcabouço normativo atualmente disponível já seria possível reconhecê-lo como prática abusiva e tratar as consequências dele advindas".

viola as práticas mercadológicas responsáveis, contraria o princípio da boa-fé objetiva na relação e agrava a vulnerabilidade do consumidor, conforme será visto no capítulo 3 do presente estudo.

No Brasil, o Projeto de Lei (PL) 281/2012, atual 3514/2015[44], e a Lei 14.181/2021[45], combatem diretamente o assédio de consumo. A Lei 14.181/2021, no seu artigo 54-C, veda o assédio de consumo na oferta de crédito, principalmente aos considerados hipervulneráveis. Já o Projeto de Lei 3514/2015 propõe-se a ampliar o rol de direitos básicos do consumidor.

Para Rodrigues (2019, p. 167), embora tenha havido uma evolução com a inclusão do assédio de consumo como prática abusiva nos projetos supramencionados, eles "não tratam do assédio de forma mais específica ou aprofundada, mas sim *en passant*".

Para Catalan e Pitol (2017, p. 147), essas práticas, consideradas como assédio de consumo, ocorrem nas seguintes situações:

> a) nas repetidas visitas ao domicilio do consumidor, (b) no *spam*, (c) no assédio a idosos nas filas dos bancos, com sedutoras ofertas de crédito ou com a possibilidade de vir a ser premiado, (d) no persistente contato – via telefone, fax, *email* ou qualquer outro mecanismo de comunicação – visando a comercialização de algum bem, serviço ou a concessão de crédito, (e) na reiteração da necessidade de alteração do regime contratual vigente, (f) na extorsão das crianças para que convençam adultos a comprar-lhes algo, (g) nas promessas de cura dos mais distintos males reverberadas pela mídia etc.

A publicidade direcionada, com base em dados pessoais, caracteriza nítido assédio de consumo pela indicação de produtos e serviços, por vezes de forma repetida, conforme gostos, necessidades e interesses do consumidor, além de explora a irracionalidade e a compulsão. Utiliza as próprias características do consumidor para persuadi-lo a consumir. Não é coincidência a notificação recebida de um aplicativo sobre a promoção de alimentos após qualquer indicação de fome pelo consumidor[46]. Menos ainda a apresentação no *feed* de uma rede social de um produto ou serviço anteriormente pesquisado. São consequências das técnicas de *microtargeting* que geram o diálogo por meio da publicidade direcionada.

---

[44] "Art. 6.º [...] XII – a liberdade de escolha, em especial frente a novas tecnologias e redes de dados, vedada qualquer forma de discriminação e assédio de consumo". O PL, cujo número de origem é 281/2012, altera o CDC para aperfeiçoar contratos internacionais comerciais e de consumo. Encontra-se na Mesa Diretora da Câmara dos Deputados.

[45] "Art. 54-C. É vedado, expressa ou implicitamente, na oferta de crédito ao consumidor, publicitária ou não: [...] IV – assediar ou pressionar o consumidor para contratar o fornecimento de produto, serviço ou crédito, inclusive a distância, por meio eletrônico ou por telefone, principalmente se se tratar de consumidor idoso, analfabeto, doente e em estado de vulnerabilidade agravada ou se a contratação envolver prêmio". A Lei, recentemente aprovada em 02 de julho de 2021, altera o CDC para inserir uma seção para proteção e combate ao superendividamento.

[46] O Ifood trabalha diretamente com técnicas de segmentação. Identifica os gostos do consumidor individualmente, opera seus cupons e promoções conforme esse detalhamento, bem como utiliza a linguagem da notificação com base em cada público (A ESTRATÉGIA..., 2019).

Cumpre observar que, embora as redes operem de forma coletiva, cada um, individualmente, vive um mundo virtual paralelo, segmentado, especializado, conforme algoritmos de processamento de dados. Como se viu no subseção 2.1 do presente estudo, ao utilizar o ambiente virtual, as técnicas de coleta, tratamento e difusão, os consumidores agem de forma conjunta ensejando o assédio de consumo pela publicidade direcionada. O consumidor de vidro é constantemente persuadido pelo assédio do seu próprio eu, que se converte em informações.

2.4 A reconfiguração dos atores que compõem a publicidade direcionada: o novo consumidor e o fornecedor

Os negócios que envolvem a disponibilização e o acesso a dados pessoais são, aparentemente, gratuitos porque contrariam a tradicional realização da relação jurídica no que diz respeito à contraprestação pecuniária direta. No entanto, são suportados pelo financiamento da publicidade direcionada. O consumidor é a própria mercadoria quando se observa a economia de dados, uma vez que são as suas informações que servem de engrenagem vital para a economia[47].

Segundo Konder e Souza (2019), para que um contrato seja considerado oneroso, é necessário verificar as vantagens e os sacrifícios das partes, o que não implica um nexo de reciprocidade obrigacional. A onerosidade depende da qualidade de qualquer sacrifício, ainda que não esteja relacionada com o serviço apresentado no contrato. Mesmo que não haja a identificação clara de remuneração direta, existem os casos com "gratuidade aparente" em que, embora não seja exigida diretamente do consumidor a prestação, o fornecedor obtém vantagem em razão dessa relação, o que ocorre nitidamente na economia de dados pessoais (KONDER; SOUZA, 2019).

No mesmo sentido, Bioni (2020a, p. 24, grifo do autor) afirma:

> Traçando um paralelo com outras operações econômicas, cuja contraprestação pelo bem de consumo é fixada pecuniariamente, sabe-se exatamente o custo de transação caracterizado por um *deslocamento patrimonial*, enquanto na lógica da economia informacional, é incerto como a disponibilização de uma informação pessoal poderá afetar o seu titular e, por conseguinte, o 'preço' a ser pago pelo bem de consumo.

A terminologia *zero-price advertisement business model* estabelece de forma clara o modelo em discussão: o consumidor não paga uma quantia determinada pelo produto ou

[47] No mesmo sentido, o modelo de negócio Freemium (sem custo + prêmio), apesar de aparentemente gratuito, é um chamariz mercadológico para a realização de novos negócios. Trata-se de uma estratégia de *marketing* para criar uma marca empresarial.

serviço, mas a contraprestação será realizada indiretamente pela venda dos dados pessoais coletados (BIONI, 2020a). O próprio consumidor, com o direcionamento publicitário, participa do ciclo mercadológico do bem, como matéria-prima e destinatário final. Nesse sentido, o negócio binomial tradicional não se insere nesse tipo de modelo uma vez que diversos atores participam da relação consumerista.

Os anúncios publicitários estão vinculados não a *websites*, mas à navegação dos usuários. Os *players* agem de forma cooperativa para direcionar a mensagem publicitária e criar perfis de consumo. Conforme Bioni (2020a), na prática, é possível realizar o direcionamento publicitário por redes (*ad networks*) conectadas por milhares de veículos (*publishers*) ao anunciante (*advertiser*). Os veiculadores publicitários (*publishers*) terceirizam a venda dos seus espaços publicitários ao anunciante (*advertiser*) para a promoção de um produto ou serviço[48]. Há outros inúmeros atores relacionados com a publicidade direcionada na *web*.

A terceirização da comercialização dos espaços publicitários possibilita o rastreamento do consumidor por meio de tecnologia de coleta, processamento e circulação para criar uma arquitetura da navegação e, consequentemente, o perfil comportamental. A sobreposição das redes de publicidade pelo acúmulo de maior quantidade dados gera o *data broker*. *Data brokers*[49] são intermediários que coletam informações pessoais dos consumidores de variadas fontes para vendê-las ou cedê-las a outras empresas. São empresas que normalmente não participam da relação de consumo tradicional; muitas vezes, o consumidor desconhece a sua existência e sua prática. Para a Federal Trade Commission (2014), os *data brokers* compilam informações dos consumidores de outras empresas com o principal objetivo de traçar perfis a fim de direcionar a publicidade. Tal tratamento de informação normalmente não é informado ao consumidor, que tem seus dados coletados, manipulados e compartilhados sem seu conhecimento e, consequentemente, sem seu consentimento. Trata-se de um ciclo informacional obscuro na relação, que influi diretamente no êxito do negócio.

Figura 2 – Ciclo mercadológico por meio de *data brokers*.

[48] Como exemplo, o *Real Time Bidding* (RTB) é um modelo de mídia programática na internet que funciona por intermédio de determinados atores inexistentes na mídia tradicional. Os veículos (*sites* ou aplicativos) disponibilizam seus espaços publicitários abertos por meio do *software* conhecido como *Supply-Side Platforms* (SSP). As *ad exchanges* (redes de anúncios) recebem o pedido através do SSP e oferecem aos possíveis compradores (anunciantes e agências de publicidade) sua proposta de *Demand-Side Platforms* (DSP). Uma *ad exchange* cruza os lances de DSP, indicando a melhor proposta para anunciar nos espaços disponibilizados pelos veículos. Google utiliza tal modelo, considerado como um leilão *on-line* (LEVY, 2009).

[49] Para a Federal Trade Commission (2014, p. i), "data brokers collect personal information about consumers from a wide range of sources and provide it for a variety of purposes, including verifying an individual's identity, marketing products, and detecting fraud. Because these companies generally never interact with consumers, consumers are often unaware of their existence, much less the variety of practices in which they engage".

Fonte: Elaboração da autora.

Com novos atores, é possível afirmar que o conceito de fornecedores na relação discutida deve ser ampliado. O artigo 3.º[50] do CDC enuncia um rol exemplificativo. Por outro lado, para Blum (2018), Benjamin, Marques e Bessa (2013), a expressão "mediante remuneração" deve ser interpretada de forma ampla a fim de incluir o ganho indireto do fornecedor.

Equipara-se ao fornecedor aquele intermediário da relação de consumo. Como exemplo, podem-se citar as plataformas virtuais na economia colaborativa. São consideradas provedoras de aplicação, conforme o artigo 15 da Lei n.º 12.965/2014, e responsáveis em caso de vício ou defeito do produto e/ou serviço (VERBICARO; VIEIRA, 2020a). A LGPD criou ainda as figuras do controlador e do operador de dados pessoais, que serão responsabilizados em caso de uso indevido ou ilícito, conforme será visto no capítulo 4.

É fato, portanto, que o *zero-price advertisement business model* é uma complexa forma de realização de negócio por intermédio de novos atores, por vezes desconhecidos pelo consumidor, para criação de perfis com a finalidade de direcionar a publicidade, com base no perfil comportamental, para persuasão ao consumo de bens e/ou serviços. Afirmar que a

[50] "Art. 3.º. 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.º Produto é qualquer bem, móvel ou imóvel, material ou imaterial. § 2.º 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".

ausência de onerosidade desqualifica a relação de consumo é uma grande falácia. Nessa relação, o consumidor, além de participar de todo o ciclo mercadológico como destinatário final do bem de consumo por meio da publicidade direcionada, torna-se a própria mercadoria quando disponibiliza seus dados pessoais para ter acesso a uma plataforma.

3 *E-COMMERCE*, DADOS PESSOAIS E RELAÇÕES DE CONSUMO: UMA ANÁLISE DAS CARACTERÍSTICAS DO CONSUMO NO COMÉRCIO ELETRÔNICO

Nos últimos anos, a superação do consumo analógico pelo digital foi crescente e constante, tendo sido acelerada pelas medidas restritivas impostas em razão da pandemia de Covid-19. No entanto, é primordial entender a caracterização desse comércio e de seus agentes.

Marques (2004a) define comércio eletrônico de maneira estrita e ampla. No primeiro caso, o comércio eletrônico diz respeito a contratações não presenciais ou a distância no meio eletrônico ou por via eletrônica. De forma ampla, é um novo modelo de negócio concretizado por meio de um sistema de redes eletrônicas, o que abrangeria todas as formas de transação e de troca de informações comerciais, baseadas na transmissão de dados, englobando "atividades negociais, juridicamente relevantes, prévias e posteriores à venda ou à contratação" (MARQUES, 2004a, p. 38).

Lucca (2003, p. 33) faz distinção entre contrato informático – negócio jurídico bilateral que tem por objeto bens e serviços vinculados à ciência da computação – e contrato eletrônico – aquele celebrado no ambiente do computador ou de redes de comunicação.

Assim, o contrato eletrônico não é um novo tipo de contratação, é uma exigência instrumental em razão da globalização e do desenvolvimento tecnológico (VERBICARO; MARTINS, 2018, p. 2-3). A contratação eletrônica pode ser "entendida como contratação em rede, no âmbito de uma loja virtual, ou contratação em linha, sem negociação entre as partes, ou, ainda, contratação por meio de comunicação individual, através de meios eletrônicos" (FARIAS; ROSENVALD, 2013, p. 335).

Miragem (2019b, p. 22) afirma:

> O comércio eletrônico de consumo observa grande crescimento no direito brasileiro, dadas as facilidades que permite, como a possibilidade de adquirir produtos e serviços sem ter de deslocar-se até o estabelecimento físico do fornecedor, ou a comparação de preços entre diferentes fornecedores. Por outro lado, entre as desvantagens do sistema estão limitações de contato direto e pessoal entre o consumidor e o produto no momento da aquisição – o que atrai a utilidade da incidência do art. 49, assegurando o direito de arrependimento do consumidor – assim como a vulnerabilidade inerente à forma da contratação, tanto para efeito de acesso à informação sobre o contrato, controle dos meios de pagamento e a própria localização geográfica do fornecedor, por vezes submetido à jurisdição estrangeira (no caso do comércio eletrônico internacional).

Schreiber (2014, p. 4) sustenta que a contratação eletrônica é aquela efetivada no ambiente eletrônico. Para o autor, não há necessidade de criação de um novo gênero contratual, a contratação eletrônica seria uma maneira diversa dos contratos já tipificados, seja pelas

transformações no modo de celebração, seja pelo desenvolvimento da relação jurídica entre os contratantes[51].

Segundo Lorenzetti (2004, p. 274-275), as novas formas eletrônicas de contratação estão eivadas de problemas: a) desumanização do contrato; b) imputabilidade da declaração de vontade, o que se reflete na sua forma e na sua validade; c) distribuição de riscos dessa declaração; d) formação do consentimento; e) competência; f) diferentes graus de utilização do ambiente virtual. A imputabilidade da declaração de vontade está relacionada com a falta do real conhecimento sobre a contratação, que exteriorizada por meio de códigos binários, códigos eletrônicos de difícil compreensão.

Miragem (2019b) destaca a ampliação das formas de contratação no ambiente virtual. Houve uma mudança de paradigma na relação jurídica pelo estabelecimento de maneiras atípicas de contratação, especialmente quando se consideram as plataformas eletrônicas, os contratos inteligentes e os novos tipos de produtos e serviços.

A plataforma eletrônica é normalmente a intermediadora da relação jurídica; por isso, não poderia ser considerada um fornecedor em si, mas um facilitador do negócio a ser realizado:

> O fornecimento de produtos e serviços por intermédio de plataforma digital conta com uma estrutura característica da relação jurídica que se estabelece entre três pessoas distintas: a) o organizador da plataforma, que intermedeia a relação; b) o fornecedor direto do serviço; c) o consumidor. O organizador da plataforma é aquele a quem incumbe definir o modelo do negócio e do modo como produtos ou serviços serão ofertados e fornecidos por intermédio da internet (MIRAGEMb, 2019, p. 22).

No entanto, esse dito guardião de acesso poderá ser responsabilizado pela legislação consumerista de acordo com o seu grau de intervenção na relação, podendo ser solidariamente responsável quando caracterizada a cadeia oculta de todos os fornecedores envolvidos na relação. Ainda, as plataformas digitais são responsáveis pelas informações veiculadas na sua plataforma[52] e pelas situações que envolvam práticas discriminatórias, como exclusão do consumidor, por meio do *geoblocking* e do *geopricing*[53] (subseção 2.2.1).

---

[51] Para Schreiber (2014, p. 4-5), é um verdadeiro calvário para o legislador e para os tribunais definir quem contrata, onde contrata, quando contrata, como contrata e o que contrata no ambiente eletrônico.

[52] É importante frisar que o Superior Tribunal de Justiça (STJ) já consolidou o entendimento sobre a responsabilidade solidária entre aqueles que veiculam a publicidade enganosa e os que a aproveitam na comercialização do produto ou serviço, em observância ao direito à informação para assegurar ao consumidor escolhas conscientes, bem como os deveres anexos de lealdade, confiança, cooperação e proteção (CARVALHO, FERREIRA, 2017, p. 714-716).

[53] Afirma Miragem (2019b, p. 8): "Outro aspecto a ser considerado, à luz do direito do consumidor, serão as situações de bloqueio ou exclusão do consumidor do ambiente de negócios viabilizado pela plataforma digital que tenha acesso controlado (e.g. mediante cadastro prévio, uso de senha, etc.), hipótese em que a decisão do organizador, automatizada ou não, submete-se aos limites definidos pela proibição de práticas abusivas, em especial as previstas no art. 39, incisos II ('recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes') e IX ('recusar a venda

Os contratos inteligentes – *smart contracts* – são aqueles que se submetem a programações automáticas e executáveis no ambiente digital, totalmente ou parcialmente, com agentes distintos dos fornecedores e consumidores como executores de ações específicas ou destinatários (MIRAGEM, 2019b, p. 8-9). O sistema *hCaptcha*, usado nas votações dos "paredões" no programa televisivo *Big Brother Brasil*, é um *smart contract* que pode gerar crédito para o grupo Globo Comunicações e Participações S.A. por meio de criptoativos[54]. A remuneração em *Human Tokens*[55] será determinada conforme as cláusulas contratuais.

É importante frisar que a constituição do ambiente virtual alterou produtos e serviços. Bens, antes concretamente materiais, transformaram-se em serviços[56], houve a integração de objetos-serviços, bens digitais[57] e a integração de inteligência artificial à produção de bens e serviços.

Marques (2004a, p. 61-62) afirma que a contratação eletrônica tem especificidades que a diferenciam do negócio jurídico tradicional: a) despersonalização, b) desmaterialização, c) desterritorialização e atemporalidade e d) desconfiança dos consumidores no comércio eletrônico.

A despersonalização está caracterizada na contratação realizada a distância, por meio eletrônico, em silêncio, impondo uma massificação da relação, concretizada pelos contratos de adesão, o que impossibilita o diálogo entre as partes:

> O sujeito fornecedor agora é um ofertante profissional automatizado e globalizado, presente em uma cadeia sem fim de intermediários (portal, *website*, *link*, *provider*, empresas de cartão de crédito etc.), um fornecedor sem sede e sem tempo (a oferta é permanente, no espaço provado e no público), um fornecedor que fala todas as línguas ou usa a *língua franca*, o inglês, e utiliza-se da linguagem virtual (imagens, sons,

de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais'), do CDC (LGL\1990\40)".

[54] "O proprietário do site é remunerado, primeiro, por cada resposta que os usuários do *site* dão (recompensa por resposta). Esse valor é multiplicado pela recompensa por 'respostas humanas úteis' que o site dá (recompensa pelas respostas humanas úteis). Se o proprietário utiliza um *bot* para responder ao *hCaptcha* da própria página, ele não receberá nada porque sua recompensa pelas respostas humanas úteis será zero. Finalmente, sua remuneração será determinada por um valor fixado pela *hCaptcha* de acordo com a quantidade de tarefas disponíveis na rede (razão de preenchimento ou *fill rate*). Como o *hCaptcha* não pode deixar de funcionar mesmo se nenhuma empresa tiver solicitado serviço – já que os sites dependem dele para barrar tráfego malicioso –, o sistema manda tarefas cujas respostas já são conhecidas para calibrar o sistema. A razão de preenchimento é a proporção entre tarefas solicitadas por empresas e tarefas de calibração de sistema" (KLAFKE, 2021, p. 7-8).

[55] Pacote padronizado de informações que podem ser trocadas por usuários que aceitam o Protocolo HUMANO ou servem como forma de pagamento de serviços (KLAFKE, 2021, p. 8).

[56] Pode-se citar a contratação de serviços de leitura de livros virtuais.

[57] Zampier (2017, p. 73) afirma que bens digitais são "aqueles bens incorpóreos, os quais são progressivamente inseridos na Internet por um usuário, consistindo em informações de caráter pessoal que trazem alguma utilidade àquele, tenha ou não conteúdo econômico". Segundo Paixão e Kai (2020, p. 217), "Os bens digitais patrimoniais são aqueles capazes de gerar repercussões econômicas imediatas quando são inseridos em rede, enquanto os bens digitais existenciais geram repercussões extrapatrimoniais e o tipo patrimonial-existencial une características dos dois, podendo se tornar mais comum devido à facilidade de monetização das manifestações no ambiente virtual".

> textos em janelas, textos interativos, ícones, etc.) para o marketing, negociação e contratação.
> O sujeito consumidor é agora um destinatário final contratante (art. 2.º do CDC), um sujeito 'mudo' na frente de um *écran*, em qualquer tempo, em qualquer língua, com qualquer idade, identificado por uma senha (PIN), uma assinatura eletrônica (chaves-públicas e privadas), por um número de cartão de crédito ou por impressões biométricas (MARQUES, 2004a, p. 63).

Segundo Verbicaro e Martins (2018, p. 3-4), a despersonalização mitiga a presença humana e gera efeitos problemáticos na concessão do consentimento. Isso porque os sujeitos são identificados por códigos, signos e números, e não estão situados no mesmo tempo e espaço, o que impossibilita o diálogo e a negociação[58].

É um paradoxo virtual despersonalizar o consumidor pela automatização da sua declaração de vontade, mas, ao mesmo tempo, realizar a subjetivação por meio do uso irrestrito de dados pessoais. Por isso, Valim (2019, p. 4) afirma que, embora a contratação eletrônica seja realizada de forma despersonalizada – uma vez que o consumidor dificilmente saberá essencialmente com quem está contratando –, a prestação é mais individualizada e sob medida. A consequência é a inevitável diminuição da autonomia de vontade em virtude da redução da capacidade de controle pela imposição dos contratos de adesão, pelo direcionamento de informações, pela complexidade da relação e, consequentemente, pela redução da privacidade (LORENZETTI, 2001, p. 22). Nos temos de Marques (2004a, p. 72), vive-se numa ambiguidade básica entre a "pseudo-soberania do indivíduo" e a "sofisticação do controle!".

A desmaterialização está diretamente relacionada com a inexigibilidade da forma física para a realização do negócio, pois os contratos são concluídos em códigos binários ou *bits*; com um *click*, é possível obter a adesão integral ao contrato. Marques (2004a, p. 81-87) destaca a desmaterialização da linguagem virtualizada do contrato e a dificuldade de observar a desconformidade no meio abstrato[59] como características que impossibilitam o diálogo na relação, devendo ser suprimidas pela boa-fé e pelo dever de informar, muitas vezes, inexistentes.

Em outras palavras, além de não ter acesso fisicamente ao bem, na maioria dos casos, o consumidor não tem informações qualificadas, seja sobre o bem a ser adquirido ou o serviço

---

[58] Em outro sentido, Jovanelle (2012, p. 69) destaca a incerteza da identificação do consumidor internauta, uma vez que, para aprovar a compra de um bem ou a contratação de um serviço, basta conhecer alguns dados pessoais e a numeração de um cartão de uma pessoa capaz.

[59] Para Marques (2004a, p. 86-87), "há dois tipos de desmaterialização de vícios da informação: o vício da informação *stricto sensu* (aquele identificado pela CDC, por exemplo, no art. 18, in fine, e 20, in fine, do CDC) referente à disparidade entre a informação pré-contratual da oferta ou publicidade e o 'produto' ou 'serviço' efetivamente prestado ou o contrato ou manual técnico enviado no comércio eletrônico; e o vício do produto informacional ou eletrônico, um vício de qualidade ou quantidade do produto ou serviço, que quebra a confiança do consumidor".

pretendido, seja sobre o contrato em si. O excesso informativo não pode ser equiparado à informação qualificada uma vez que a grande quantidade de informações técnicas aumenta a incerteza e o desconhecimento do consumidor sobre aquela relação.

A desterritorialização e a atemporalidade da contratação eletrônica estão diretamente relacionadas com a ausência de amarras territoriais da relação. O consumidor poderá contratar de onde e a qualquer tempo desejar. O espaço para a comunicação não é mais um fator essencial para a realização do negócio. Nesse contexto, insere-se o consumidor-comunidade global diante da crítica de limitação territorial para a proteção da categoria. Para Verbicaro e Verbicaro (2017, p. 129), o conceito de consumidor ultrapassa fronteiras nacionais e assume uma dimensão desterritorial, e um fator legítimo de discriminação é sua "vulnerabilidade econômica transnacional" ante as necessidades e relações globais.

Nessa perspectiva, mister se faz destacar o entendimento do STJ sobre a caracterização da teoria do *stream of commerce*: o fornecedor, ao ampliar seu mercado de consumidores a diversos países, deve obedecer à legislação respectiva de cada nacionalidade (SCHREIBER, 2014b, p. 95)[60].

Em relação à atemporalidade da contratação, o Decreto Federal n.º 7.962/2013 impôs o dever de confirmação[61] como forma de transcender o binômio das contratações tradicionais proposta-aceitação, além de fixar o momento da realização do negócio jurídico, evitando a insegurança do consumidor sobre a formação do contrato (SCHREIBER, 2014, p. 10-12).

A complexidade da relação contratual eletrônica gera uma insegurança no consumidor. Ainda se questiona se os direitos da personalidade e a privacidade continuarão a ser protegidos mesmo com o desconhecimento da técnica cibercontratual que possibilita a realização do negócio:

> Realmente, há uma intrínseca complexidade técnica e jurídica desse tipo de contratação à distância. Para lá do *click-agreement*, que seria contratado com um simples bater de uma tecla no lugar indicado, o comércio eletrônico é pleno de surpresas, desde contratos "encapsulados" ou *wraps-agreements*, que só são

[60] Schreiber (2014b, p. 95), ao desenvolver sobre a temática, afirma que "quem direciona seu comércio aos consumidores de certos países assume o ônus de ter sua atividade disciplinada pelas respectivas leis nacionais".

[61] Decreto Federal 7.962/2013, artigo 4°: "Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos; II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação; III - confirmar imediatamente o recebimento da aceitação da oferta; IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação; V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato; VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor; e VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor. Parágrafo único. A manifestação do fornecedor às demandas previstas no inciso V do caput será encaminhada em até cinco dias ao consumidor".

> visualizados após a contratação, contratos por série de clicks em cadeia, aos cookies presentes, desvendadores dos visitantes de determinado site ou portal, aos contratos que só são virtuais e nunca podem ser realmente "captados" e perenizados pelo consumidor, tendendo – ou facilitando – a que o fornecedor mude o conteúdo o conteúdo contratual como o passar do tempo virtual (MARQUES, 2004a, p. 97).

Para Schmidt Neto (2016), a vontade livremente manifestada não é estabelecida na contratação eletrônica uma vez que a racionalidade de comprar/contratar é mitigada pela indução da vontade. Assim, a confiança está na expectativa de obter o objeto celebrado, já que "a contratação na internet demanda fé, uma vez que não há qualquer garantia de cumprimento da obrigação, pois o consumidor não sabe nada do fornecedor, apenas espera que ele não só cumpra a sua palavra e encaminhe objeto adquirido" (SCHMIDT NETO, 2016, p. 224).

É fato que a confiança está atrelada à boa-fé: as partes acreditam nos elementos externos e no contrato em si. Segundo Schmidt Neto (2016, p. 231), a confiança e a boa-fé são dois princípios que têm pontos comuns: "um concentrado na atuação, valorando a lealdade na conduta segundo os usos do tráfico jurídico e, outro, no resultado, no reflexo social ou efeito do nascimento de direitos e deveres". No entanto, há distinção entre os dois princípios.

Nos termos de Zanchet (2006, p. 141), a boa-fé apresenta "maior grau de racionalidade das partes contratantes, estabelecendo deveres de fundo mais ético", enquanto "a confiança está mais arraigada aos fatos sociais, mais vinculada após contatos sociais, de caráter mais elementar, sem, muitas vezes, qualquer resquício de razão", correlacionados com a proteção das partes no exercício de direitos contrários aos pactuados e convencionados por elas mesmas. É a proteção contra comportamentos contraditórios, mesmo que eles possam ter embasamento jurídico[62].

No que diz respeito à boa-fé objetiva, Marques (2011b, p. 214) afirma que está ligada à formação e à execução de obrigações, "(1) como fonte de novos deveres de conduta durante o vínculo contratual, os chamados deveres anexos; 2) como causa limitadora do exercício, antes lícito, hoje abusivo, dos direitos subjetivos; e 3) na concreção e interpretação dos contratos".

Quanto à confiança, Schmidt Neto (2016, p. 235) estabelece que ela atua nas expectativas e nos vínculos gerados nos negócios jurídicos. Já a boa-fé "é um limite ético apenas no âmbito do direito e deve ser entendido como um imperativo, uma prescrição vinda do ordenamento, que, como toda norma jurídica, reflete uma escolha ética" (FRAGA, 2017, p. 427).

---

[62] Para Gonçalves (2012 *apud* Kozlovski, 2017, p. 131) são conceitos correlacionados à boa-fé: *venire contra factum proprium* – proteção contra aquele que pretende exercer posição jurídica em contradição ao pactuado; *suppressio* – após determinado tempo, um direito não pode mais ser exercido para não contrariar a boa-fé; *surrectio* – nascimento de um direito ante a prática constante de determinados atos; *tu quoque* – proíbe que se faça contra a outra parte ato que não se faria contra si.

Para Vial (2013, p. 234), a confiança, a informação e a boa-fé, se exercidas de forma conjunta, geram o equilíbrio contratual, e a transparência é o alicerce dos direitos e deveres na busca da harmonia da relação.

Em outra perspectiva, a realização da contratação eletrônica tem por base o que é visto em detrimento do que é lido ou entendido (MARQUES, 2004a, p. 82). O consumidor acredita na boa aparência e na "marca" daquilo que está adquirindo, buscando, muitas vezes, a real identificação e qualificação do seu fornecedor quando o produto apresenta defeitos[63] (SCHREIBER, 2014, p. 6).

Há uma caracterização da hiperconfiança no comércio eletrônico pelas vulnerabilidades intrínsecas da relação, além de extensas condições gerais de contratos impostas ao consumidor sob a forma de contratos de adesão, a não aceitação de tais termos implica a inutilização do serviço ou da compra do produto. Verbicaro e Martins (2018, p. 6) explicam:

> À medida que o acesso à Internet se torna cada vez mais natural e democratizado e a confiança nas transações online cresce consideravelmente, mais pessoas tornam-se vinculadas às mais variadas espécies de contrato sem que ao menos percebam a multiplicidade de relações jurídicas com as quais acordaram, tampouco seus respectivos termos.

Para Canto (2013, p. 198-199), a dinamicidade do ambiente impõe um panorama de vulnerabilidade agravada e de desconfiança aos agentes da relação. Verbicaro e Vieira (2020a) evidenciam tais características ao analisarem os termos da contratação de serviço via plataformas, especialmente por meio do Airbnb. Pode-se contratar a qualquer tempo e lugar, mas sem a certeza dos atores envolvidos e da caracterização do imóvel alugado. É uma expectativa de direito que será confirmada ou não com a chegada do consumidor ao imóvel objeto da transação.

Nesse sentido, Canto (2014, p. 22) considera que há um agravamento da vulnerabilidade do consumidor inserido nesse contexto de contratação em decorrência da desmaterialização e da ubiquidade do ambiente. O fornecedor sem face obtém informações do consumidor em seu ciclo de movimentação na *web*.

Quando se analisam as relações de consumo realizadas por influência da publicidade direcionada obtida pela modulação algorítmica de dados pessoais, observa-se uma concreta redefinição do modelo de massificação das demandas de consumo, com uma individualização

---

[63] Para evitar essa insegurança relacional causada pela despersonalização, o Decreto Federal n.º 7.962/2013, no seu artigo 2.º, determina: "Art. 2.º Os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações: I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda; II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato […]".

exacerbada do consumidor. Nesse sentido, a vulnerabilidade inerente à relação ganha novos moldes:

> A vulnerabilidade se torna a expressão inexorável dessa relação entre desiguais desde a formação das sociedades de consumo massificadas. Entretanto, esse princípio fundador das leis protetivas do consumidor, quando inserido no contexto do acelerado desenvolvimento tecnológico e da virtualização das relações jurídicas, alcança patamares antes inimagináveis pelo legislador brasileiro no momento da elaboração do Código de Defesa do Consumidor na década de 90 (CANTO, 2014, p. 52).

As transformações das relações consumeristas exigem estudo e interpretação que abarquem as novas situações mercadológicas (MIRAGEM, 2019b, p. 18), especialmente quando se analisam a coleta, o tratamento e o uso de dados pessoais, tendo como pressuposto a (hiper)vulnerabilidade do consumidor – que pode ser informacional, comportamental, algorítmica e situacional, conforme será explanado nas subseções seguintes.

3.1 A vulnerabilidade do consumidor agravada na contratação eletrônica e na economia de dados pessoais

Todos têm o direito de ser iguais quando a diferença inferioriza e diferentes quando a igualdade descaracteriza (SANTOS, 2003, p. 56). O reconhecimento da vulnerabilidade segue essa premissa. A pós-modernidade é marcada pelo reconhecimento da diferença e da desigualdade. Nessa perspectiva, o direito à igualdade desvinculou-se do caráter meramente formal, ou seja, da forma da lei, para fundar-se em critérios materiais. Como reflexo dessa mudança, os indivíduos passaram a ser tratados de maneira diversa em busca do ideal de igualdade. São caracterizados como vulneráveis os que têm necessidade de um tratamento diferente diante da busca do equilíbrio e da equiparação nas relações (MARQUES; MIRAGEM, 2012, p. 125).

Para Konder (2015, p. 103), a vulnerabilidade tem por finalidade proteger a dignidade da pessoa humana com base no princípio constitucional da solidariedade social. A proteção dos vulneráveis pelo direito tem sua origem na identificação da situação de desigualdade, construindo-se, a partir dessa premissa, um sistema de normas e subprincípios orgânicos de reconhecimento e efetivação de seus direitos (MARQUES; MIRAGEM, 2012, p. 125). No direito privado, o reconhecimento da vulnerabilidade tem por fundamento a igualdade no combate da não discriminação, possibilitando não apenas o reconhecimento da diferença, mas também o exercício da liberdade de ação e da opção (MARQUES; MIRAGEM, 2012, p. 196-197).

A vulnerabilidade não significa incapacidade ou hipossuficiência[64]. Trata-se da constante propensão para sofrer danos de natureza física, psicológica e social (CANTO, 2013, p. 189). Pode-se afirmar ainda que a vulnerabilidade tem uma função social: não está ligada somente ao sujeito em si, mas ao grupo em que está inserido.

A proteção do consumidor ganhou destaque com a Constituição Federal (CF) de 1988 e foi reconhecida no direito positivo constitucional como direito fundamental. Ao inserir a defesa do consumidor no rol de direitos fundamentais (art. 5.º, XXXII), a Constituição reconhece a fragilidade do consumidor no mercado (ROCHA, 2018, p. 15).

O CDC representou um avanço na proteção do consumidor por reconhecer a vulnerabilidade além da visão econômica, devendo o Estado garantir "o equilíbrio do sistema econômico de tal forma que se limitem abusos e práticas de mercado injustas e distantes do princípio ético da boa-fé objetiva" (ROCHA, 2018, p. 19). Assim, o reconhecimento da vulnerabilidade do consumidor no artigo 4, I, do CDC é uma das bases do ordenamento consumerista brasileiro, sendo o mecanismo que alcança a igualdade material por meio dos direitos de escolha, reflexão, informação e transparência para proteger a liberdade ou a autonomia de vontade, diante do conceito de consumidor individual, difuso, coletivo em sentido *stricto* ou individual homogêneo. A base do direito consumerista justifica-se pelo reconhecimento da vulnerabilidade (MARQUES, MIRAGEM, 2012) na busca do equilíbrio na relação de consumo.

Todos os grupos de consumidores são considerados vulneráveis em razão da função social do direito privado solidário (MARQUES; MIRAGEM, 2012, p. 127)[65]. A vulnerabilidade é "inerente à condição do consumidor, seja ela técnica, econômica, jurídica, seja psicológica" (EFING, CAMPOS, 2018, p. 152). No mesmo sentido, Milhomens (2021, p. 138-139) assevera:

> No contexto de consumo, a vulnerabilidade é comumente associada a um estado de preocupação, fragilidade, dificuldade de autoproteção ou de estar em risco, que pode expor o consumidor a danos econômicos, físicos ou psicossociais nas interações com o ambiente mercadológico ou de consumo de mensagens de marketing ou produtos.

---

[64] Para Chazal (2000, p. 1-2), vulnerável é a pessoa ou coisa que pode ser ferida, lesionada. De fato, em um primeiro sentido, a palavra latina *vulnus* significa ferida, isto é, lesão corporal; mas, mesmo em latim clássico, *vulnerare* logo se reveste de um sentido figurado. Portanto, a ideia de lesão potencial, não somente física, mas também psíquica, deve ser privilegiada.

[65] Pode-se afirmar, na mesma linha, que o trabalhador é vulnerável em razão das condições pessoais e dos riscos laborais. Alves (2019, p. 120) conceitua a vulnerabilidade laboral como a "situação de inferioridade contratual agravada por fatores de risco laboral ou pela condição pessoal do trabalhador, seja ele empregado ou não, que poderá resultar em lesão em sua esfera patrimonial ou existencial". Vulnerabilidade, no entanto, não se confunde com subordinação. A subordinação significa a prestação de serviço de forma dirigida, o empregado seguindo as orientações e determinações dentro de limites legais (GARCIA, 2012, p. 65). De acordo com esses conceitos, o trabalhador pode ser vulnerável sem ser empregado ou subordinado juridicamente.

A vulnerabilidade do consumidor está na sua própria condição existencial[66]. Segundo Marques (2011a, p. 322), a vulnerabilidade pode ser um conceito legal e indeterminado, com muitos sentidos e muitos efeitos práticos. Segundo Baker, Gentry e Rittenburg (2005, p. 129), alguns conceitos de vulnerabilidade focam características ou limitações individuais, outros, condições externas e/ou a interação entre fatores internos e externos. Considerando-se aspectos econômicos, técnicos e pessoais[67], pode haver diversas subespécies de vulnerabilidade.

A fluidez e a flexibilidade do enquadramento do consumidor como categoria (CHAZAL, 2000) estendem-se ao diagnóstico da vulnerabilidade, uma vez que o contexto e subjetividades definirão o agravamento dessa condição. Nesse prisma, a vulnerabilidade é relacional, quando o consumidor está em uma situação de inferioridade na relação com o fornecedor; é provável[68] e variável, daí se falar em situação de vulnerabilidade[69] (CHAZAL, 2000, p. 6-9):

> [...] o consumidor passa, na realidade, de uma situação de vulnerabilidade, ou seja, de uma potencial lesão de seus interesses, para uma situação de dificuldades comprovadas. É o caso quando a situação de superendividamento das pessoas físicas é caracterizada '*pela manifesta impossibilidade para o devedor de boa-fé de enfrentar o conjunto de suas dívidas não profissionais vencidas e vincendas*' (L 331- 2 do C. Cons.). Para lidar com essa situação de superendividamento, medidas específicas de planejamento, de extensão e de redução das dívidas devem ser tomadas a favor do consumidor (CHAZAL, 2000, p. 8, grifo do autor, tradução nossa)[70].

Segundo Barocelli (2017, p. 53), a vulnerabilidade será agravada ou especificada, conforme condições (a)temporais de cada categoria e situação, o que possibilita um aprofundamento fático e jurídico da relação existente – empregado, consumidor ou não enquadrado na conceituação específica (ALVES, 2019, p. 123). São as ditas vulnerabilidades

---

[66] Cumpre destacar a concepção de vulnerabilidade estrutural nas relações de consumo defendida por Milhomens (2021, p. 179), como uma vulnerabilidade de *status* da própria condição de consumidor que atrai a sua caracterização.

[67] Marques e Miragem (2012) apresentam como vulnerabilidades intrínsecas dos consumidores a vulnerabilidade técnica, a jurídica, a fática e a informacional. Ainda, conforme Verbicaro, Vieira (2021b), o consumidor será considerado vulnerável conforme a análise de suas características subjetivas e do caso concreto, como a mulher no assédio discriminatório de gênero.

[68] Afirma Chazal (2000, p. 7): "Il faut rappeler que la protection du consommateur ne se justifie que par son état de vulnérabilité, c'est à dire de victime potentielle, sans que la commission d'un abus effectif soit, en principe, exigé comme préalable. Le droit de la consommation s'articule donc autour d'une double probabilité: une double probabilité: d'une part, il est probable que le consommateur se trouve en situation d'infériorité par apport au professionnel et, d'autre part, il est probable que la personne en position dominante ait tendance à en abuser au détriment de celle qui se trouve en position vulnérable".

[69] A situação de vulnerabilidade está relacionada ao potencial lesivo da condição econômica e geográfica do consumidor (CHAZAL, 2000, p. 8).

[70] No original: "[...] le consommateur passe, en réalité, d'une situation de vulnérabilité, c'est-à-dire d'une lésion potentielle de ses intérêts, à une situation de difficultés avérées. Tel est le cas lorsque la situation de surendettement des personnes physiques est caractérisée '*par l'impossibilité manifeste pour le débiteur de bonne foi de faire face à l'ensemble de ses dettes non professionnelles exigibles et à échoir*' (L 331- 2 du C. Cons.). Pour traiter cette situation de surendettement, des mesures particulières d'aménagement, d'étalement et de réduction des dettes doivent être prises en faveur du consommateur".

relacionais que serão variáveis ou prováveis (CHAZAL, 2000), conforme a análise específica de cada categoria de consumidor.

Para Barocelli (2017, p. 53), ao enquadrar uma categoria como hipervulnerável, é necessário entender as subjetividades do grupo e o normativo legal a ser aplicado. De acordo com a doutrina consumerista, a condição de hipervulnerabilidade depende da "situação social, fática e objetiva de agravamento da pessoa física consumidora por circunstâncias pessoais ou aparentes conhecidas do fornecedor" (MARQUES; MIRAGEM, 2012, p. 201). Essa condição, portanto, poderá ser permanente ou temporária conforme o caso a ser estudado[71]. Seu grau de excepcionalidade é determinado pelo estado subjetivo multiforme e pluridimensional (MARQUES; MIRAGEM, 2012, p. 202).

Segundo Marques e Miragem (2012, p. 202), categorias reconhecidas constitucionalmente como desiguais devem ser consideradas hipervulneráveis nas relações consumeristas, como os idosos, as crianças, entre outras. No entanto, além dos grupos admitidos pela lei como hipervulneráveis, a acepção foi ampliada para abarcar categorias que sofrem dano cotidiano na sociedade de consumo (VERBICARO; VIEIRA, 2020a). Barocelli (2017, p. 55) categoriza como hipervulneráveis aqueles cuja condição de desigualdade é agravada por condições temporais e atemporais, destacando as pessoas com doenças mentais ou vícios, pessoas da comunidade LGBTQIA+, grupos pertencentes a minorias, imigrantes e usuários de comércio eletrônico.

No comércio eletrônico, o consumidor está exposto ao agravamento da sua vulnerabilidade. Conforme Canto (2014, p. 52) e Chazal (2000, p. 9), como a vulnerabilidade é uma noção relativa, essa condição deverá ser analisada a partir da situação (condição) geográfica na qual o consumidor está inserido.

Chazal (2000, p. 10) afirma que tal condição está presente na contratação, quando tanto o consumidor quanto o fornecedor estão em locais geograficamente diferentes. Nessa situação, para o autor, é difícil avaliar o bem a ser adquirido e a possível caracterização de vício. No mesmo sentido, Canto (2014, p. 77-91) menciona que as próprias especificidades da contratação eletrônica – desterritorialização, despersonalização, desmaterialização, hiperconfiança e atemporalidade da relação (visto no tópico acima) – são ensejadoras do agravamento da vulnerabilidade do consumidor inserido no *e-commerce*. No entanto, deve-se atentar para as diferentes camadas da relação consumidor-fornecedor:

[71] Marques e Miragem (2012, p. 200-201) destacam que o CDC, nos seus artigos 37, parágrafo 2.º, e 39, IV, já mencionavam a noção de vulnerabilidade agravada de categorias do consumidor. A jurisprudência, consolidada pelo STJ, solidificou a expressão hipervulneráveis.

> A primeira camada é a vulnerabilidade de relação, base indispensável e inerente ao próprio direito consumerista, que reconhece deter o fornecedor uma superioridade técnica, jurídica, fática e informacional em relação ao consumidor, sendo necessário conferir instrumentos a este para defender-se e reequilibrar essa relação naturalmente desigual.
> Sobre essa vulnerabilidade basilar alicerçar-se-á a transposição das relações de consumo para o mundo online – também denominada de virtualização do real –, que passará a compor a segunda camada de vulnerabilidade.
> [...].
> Dessas duas camadas podem emergir casos de consumidores que apresentam fragilidades intrínsecas capazes de torná-los hipervulneráveis, necessitando de um tratamento especial por parte dos fornecedores e, também, por parte dos aparatos estatais legiferastes administrativos e judiciais, de maneira a aperfeiçoar a realização do princípio da igualdade.
> Note-se que nem todos aqueles que apresentam condições pessoais fragilizantes (hipervulnerabilizantes) na primeira camada as terão reproduzidas na segunda, e vice-versa, uma vez que elas manifestar-se-ão das circunstâncias do caso e da condução de boa-fé dos fornecedores (CANTO, 2014, p. 91).

Na economia de dados, a boa-fé é colocada em questão diante da assimetria da relação, tanto informacional como de controle. No comércio eletrônico, além das características atípicas em relação aos contratos tradicionais (como visto no item anterior), observa-se uma nova roupagem da contratação, por causa dos aspectos pré-contratuais, como a oferta e a publicidade direcionada, ou ainda da nova configuração de atores e da caracterização das figuras de consumidor e fornecedor, como analisado na subseção 2.5. Não se trata de um aspecto subjetivo ou de uma condição pessoal, como a do idoso, mas de um traço objetivo pela "emergência de uma nova economia que vulnera o consumidor, especialmente os seus dados pessoais, com o desenrolar de uma dinâmica própria" (BIONI, 2020a, p. 158)[72].

A personalização e a segmentação de grupos seguindo o ritmo acelerado da tecnologia informacional impõem uma desconformidade informacional à relação entre consumidores e fornecedores. Não há, de fato, diálogo real entre as partes, o que gera um dilema entre a inclusão digital e a exclusão da conectividade (LIMBERGER; SALDANHA; HORN, 2017, p. 220). Tais fraquezas acumuladas, impulsionadas pela abordagem individualizante, causam o agravamento da vulnerabilidade do consumidor no ambiente virtual, especialmente na efetivação do consentimento:

> O consumidor 'compra agora para depois'. Esse quadro de incerteza é a eloquência de uma nova vulnerabilidade na medida em que o titular dos dados pessoais pode ser 'machucado' pela má utilização de seus dados pessoais, cuja potência da 'ferida' não pode ser nem mesmo antevista.
> Somam-se, ainda, as citadas limitações cognitivas do ser humano, que o impede de calibrar as gratificações e as perdas mediatas e imediatas necessárias para racionalizar um processo de tomada de decisão genuíno a respeito do fluxo de seus dados pessoais.

[72] É importante frisar que tanto Canto (2014) quanto Bioni (2020a) identificam o agravamento da vulnerabilidade do consumidor no ambiente virtual. No entanto, há divergência no diagnóstico dessa condição: Canto (2014) foca a contratação virtual; já Bioni (2020a), volta-se para o mercado informacional. Nesta pesquisa, entende-se que tais caracterizações de agravamento de vulnerabilidade não se excluem, antes se somam.

> A situação de vulnerabilidade é maximizada por essa idiossincrasia traiçoeira do trade-off da economia informacional (BIONI, 2020a, p. 156).

Assim, há o concreto agravamento da vulnerabilidade do consumidor no ambiente virtual, especialmente na economia de dados pessoais, em razão de práticas direcionadas pelo acesso instantâneo e pela manipulação de informações pessoais dos consumidores. As práticas abusivas no direcionamento publicitário, como assédio de consumo, o desequilíbrio relacional e informacional em razão da individualização do consumidor e a ignorância ou deficiência de julgamento são condições que maximizam a vulnerabilização. Novas vulnerabilidades são diagnosticadas: informacional, situacional, psicocomportamental e algorítmica.

O estudo realizado pelas pesquisadoras Cranor e McDonald (2010), da Carnegie Mellon University, para desenhar e investigar os modelos mentais dos usuários a respeito do funcionamento da publicidade no ambiente virtual confirma as vulnerabilidades mencionadas, especialmente a informacional, a psicocomportamental e a algorítmica. Cranor e McDonald (2010) concluíram que: a) há falta de conhecimento por parte dos usuários sobre o funcionamento das tecnologias na coleta, no tratamento de dados pessoais e na formulação da publicidade; b) o controle de dados pessoais é visto pelos consumidores como um benefício, quando há um benefício imediato na relação de consumo (como, por exemplo, um desconto); c) os próprios consumidores discordam da lógica econômica e do dispêndio para assegurar a proteção da privacidade.

Um outro estudo realizado por Hoofnagle, Urban e Li (2012), da University of California, buscou investigar as tecnologias utilizadas para coletas de dados. Os autores concluíram que o mercado cria novas tecnologias de neutralização do consumidor no caso de sua capacitação para controlar seus dados (HOOFNAGLE; URBAN; LI, 2012), o que confirma a vulnerabilidade situacional do consumidor. Tais abordagens da vulnerabilidade serão delimitadas a seguir.

3.1.1 A vulnerabilidade informacional do consumidor na economia de dados pessoais

Quando se analisam as relações de consumo realizadas pela influência da publicidade direcionada, possibilitada pela modulação algorítmica de dados pessoais, observa-se que o modelo de massificação das demandas de consumo foi redefinido, havendo agora uma ênfase na individualização exacerbada do consumidor. Nesse sentido, a vulnerabilidade intrínseca da relação ganha novos moldes, podendo-se destacar a vulnerabilidade informacional, a comportamental, a situacional e a algorítmica. Não se trata da segmentação do princípio da

vulnerabilidade, mas de um alargamento do contexto relacional que impõe uma atenção especial à responsabilização.

O princípio basilar da relação consumerista é a informação, na transparência ou no reconhecimento de vulnerabilidade(s). A relação de consumo, por si só, exige o direito à informação e reconhece o desequilíbrio relacional justamente pelo desnível informativo entre os atores. Na economia de dados, é fato que essa assimetria informacional ainda é mais importante. Os consumidores não conhecem as reais características da relação eletrônica apresenta; muito menos sabem como são colhidos, tratados e dispostos seus dados pessoais, o que configura a vulnerabilidade informacional, segundo a doutrina.

É imprescindível, primeiramente, entender como se estabelece tal vulnerabilidade a partir do reconhecimento do direito à informação. Os efeitos do reconhecimento da informação como direito fundamental não se restringem à ordem privada, mas se irradiam para o campo da cidadania ativa (BARBOSA, 2019, p. 4). A CF reconhece o direito à informação e ao acesso à informação em vários artigos, como nos artigos 5.º, IV, XII, XIV, XXXIII, LX, LXXII, 37, 93, 200, 216. Destaca-se o artigo 5.º, XIV, segundo o qual "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional"; o inciso XXXIII do mesmo artigo também protege o direito à informação ao estabelecer que todos têm direito a receber dos órgãos públicos informações, sob pena de responsabilidade, ressalvado o sigilo imprescindível à segurança da sociedade e do Estado.

No que diz respeito à Administração Pública, a Constituição da República, nos seus artigos 37, parágrafo 3.º, inciso II, e 216, parágrafo 2.º, dispõe sobre o acesso à informação e o dever público de gerir documentos e franquear as informações.

Para Sarlet e Molinaro (2014, p. 12), a liberdade de informação e os direitos à informação e de acesso à informação, "além de direitos humanos e fundamentais de alta relevância, representam técnicas democráticas de alta densidade na conformação das relações humanas numa determinada comunidade política e social". Na verdade, estão ligados ao direito subjetivo de ser informado e à inata proteção dos direitos da personalidade.

Ressalvadas as distinções entre os conceitos dos direitos citados, pode-se afirmar que a informação tem uma função pública no sentido de não ser apenas um elemento de direito subjetivo, é também um direito-dever cujo objetivo é satisfazer o direito que os indivíduos têm de receberem a informação. Em sua evolução ao longo dos anos, a informação tornou-se uma espécie de garantia supranacional da democracia e de efetivação de direitos (SARLET; MOLINARO, 2014, p. 16).

Nas relações de consumo, de acordo com o artigo 6.º, III, do CDC, cabe ao fornecedor a obrigatoriedade de manter o consumidor informado (NUNES, 2017). O direito à informação é um dos pilares das relações de consumo em razão da necessidade da existência de confiança entre as partes e da caracterização de boa-fé. Assim, a informação deve estar presente em todas as fases do contrato: pré-contratual, contratual e pós-contratual, conforme os artigos 6.º, III, 30 e 31 do CDC (VIAL, 2013, p. 233).

A boa-fé objetiva é uma das bases do dever informativo. Tem como fundamento a lealdade e a confiança recíproca entre as partes em atenção a um fim comum. É um conjunto de comportamentos éticos aferidos objetivamente durante a relação contratual (GARCIA, 2015, p. 6), sendo, inclusive, uma das formas de cumprimento da cooperação entre as partes na relação.

O princípio da transparência é outro princípio ensejador do dever de informar no sentido de que a relação de consumo deve ser clara, direta, correta e de fácil conhecimento, ou seja, o consumidor precisa ter prévio conhecimento do que irá contratar ao demonstrar sua intenção em se vincular a uma relação consumerista. Assim, a informação tem o papel de preparar o consumidor para o ato de consumo verdadeiramente livre, sem vício no consentimento, fundamentado de forma adequada e completa (NUNES, 2017, p. 509).

No artigo 31 do CDC, confirma-se a preocupação do legislador de enfatizar que toda oferta e apresentação de produtos deve fornecer informações “corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem”.

Além do equilíbrio no desenvolvimento da relação em si, o acesso à informação reflete-se na proteção da saúde física e psíquica do consumidor uma vez que a desinformação possibilita a ocorrência de dano (VERBICARO; ATAÍDE, 2017, p. 79).

A desinformação, porém, está relacionada não com a completa ausência de informação, mas com informações claras, completas e compreensíveis sobre o produto e/ou serviço. Verbicaro e Ataíde (2017, p. 79) confirmam que “não é suficiente a mera disponibilidade da informação. Mais do que isto, é necessário que ela permita o processamento e a compreensão do seu conteúdo pelo consumidor menos instruído”. Assim, caso haja uma quantidade de informação técnica distante do conhecimento cotidiano, o consumidor não terá condições de entender a realidade.

Para Catalan (2019, p. 1159), a defesa da essencialidade das informações tem por base a garantia de orientação, esclarecimento, explicação, elucidação, ilustração, aclaração, explanação, iluminação, recomendação e aconselhamento dos consumidores sobre “o uso, acondicionamento, validade, riscos e (ou) de outras tantas peculiaridades fundidas àquilo que

lhes é oferecido em todo processo". Para o autor, portanto, o dever de informar consiste em decodificar de forma clara e verossímil os riscos assumidos quando se pactuou o contrato (CATALAN, 2019, p. 1159).

Para Verbicaro e Freire (2018, p. 12), o acesso à informação adequada é fundamental para a conscientização individual, para a realização de escolhas livres. Dessa forma, o consumidor, mesmo que indiretamente, extirpa aos poucos fornecedores desleais e torna-se um consumidor consciente, exercendo sua cidadania em prol da coletividade. Nesse sentido, a informação, mais que um dever, é um mecanismo de controle, uma vez que a informação disponibilizada está diretamente vinculada ao contrato, nas fases pré-contratual e pós-contratual (VERBICARO; ALCANTARA, 2017, p. 14).

Não se pode negar que a desqualificação informativa é um dos principais motivos da ocorrência de acidentes de consumo pela má utilização do produto ou serviço, sendo, inclusive, excludente de ilicitude a comprovação do fiel cumprimento do dever de informar (CATALAN, 2019, p. 1159). Além do dano subjetivo e individual, o descumprimento do dever de informar desrespeita o consumidor em caráter coletivo por violar um direito fundamental e por impossibilitar o exercício sem vício do consumo, a participação ativa e o equilíbrio mercadológico.

Quando se analisam as relações consumeristas com o avanço das tecnologias, observa-se a existência de um abismo informativo. No que diz respeito ao acesso a dados com finalidade do direcionamento publicitário, ocorre dano informativo quando há ocultamento da intenção negocial. Para Barbosa (2019, p. 7), o dano informativo decorre da ausência de informação e, consequentemente, do vício de consentimento. A informação pode ser, "propositadamente, solapada pelo fornecedor (nos casos em que a atenção do consumidor é, pelo uso de diversas técnicas de marketing, direcionada totalmente para o conteúdo publicitário)".

No que concerne às técnicas de *microtargeting*[73], a coleta de dados dá-se por meio de contratos de adesão com cláusulas difíceis, técnicas e, com frequência, em outro idioma, o que implica o vício de consentimento do consumidor, que, por vezes, não sabe de fato o que está contratando, prevalecendo a ignorância, a deficiência de julgamento e a falta de compreensão do modo como são utilizados seus dados (VERBICARO; MARTINS, 2018, p. 5).

Para Bioni (2020a, p. 154-159), a hipervulnerabilidade informacional do consumidor é resultado da complexidade do fluxo de informações, seja pela assimetria informacional, seja

[73] *Vide* Capítulo 2.

pela ausência de conhecimento técnico sobre a engenharia tecnológica dos modelos de tratamento e de coleta de dados pessoais.

Nesse sentido, o exercício da autonomia de vontade e a consequente liberdade nas relações de consumo estão diretamente ligados ao acesso à informação. A ausência informacional e ainda o excesso informativo sem qualidade caracterizam o vício de consentimento, uma vez que a vontade é fortemente relacionada com a profundidade, a coerência e a claridade informativa, como se verá na subseção 3.3 e no capítulo 4.

Há, portanto, um inexorável agravamento da vulnerabilidade quando o consumidor é inserido no mercado informacional, marcado por uma constante assimetria informativa. O dano deve-se à ausência de entendimento concreto para o exercício do consentimento ativo, a disposição de seus dados pessoais involutária e também à obscuridade do negócio. O consumidor não toma ciência de que seus dados serão utilizados como incentivo ao consumo por estratégias de *marketing*.

3.1.2 A vulnerabilidade psicocomportamental

A vulnerabilidade comportamental relaciona-se com o reconhecimento da humanidade e das limitações do consumidor contemporâneo que busca um estilo de vida ideal, padronizado pelo mercado (OLIVEIRA; CARVALHO, 2016, p. 196), em que impera o consumo. Nesse estilo de vida, os bens e serviços são considerados uma forma de poder, de diferenciação social, de segurança e de beleza e são transformados pelo consumidor em objeto de seus desejos[74]. Diante de *insights* incentivadores ao consumo, o consumidor manifesta uma fragilidade cognitiva e comportamental (OLIVEIRA, CARVALHO, 2016, p. 198).

O *marketing*, ao descobrir os desejos e estudar os comportamentos dos clientes, recorre a técnicas para conduzir comportamentos, explorar impulsos e emoções. Na economia de dados, a publicidade dirigida, com suas práticas assediadoras de consumo, torna-se sedutora, induzindo a falsa sensação de "liberdade de expressão, causando assim, sentimentos de conforto, acolhimento, bem-estar e prazer que não são encontrados nas mídias tradicionais" (PARCHEN, FREITAS, MEIRELES, 2018, p. 338).

O assédio de consumo visa influenciar o comportamento do consumidor por meio da manipulação das vontades e da compulsão ao consumo. Daí a utilização de aspectos

[74] Oliveira e Carvalho (2016, p. 184-194) apresentam como a economia comportamental (Escola de Chicago) utiliza heurísticas e *insights* comportamentais para atuar na irracionalidade do consumidor, na escolha no ato de consumo, condicionado por variáveis, de caráter emocional ou financeiro.

psicológicos, o que provoca vulnerabilidade. Miller (2012, p. 108-114) afirma que os consumidores estão sujeitos a um narcisismo consumista, que os leva a agir impulsivamente na compra de bens para não serem excluídos. Explicitam Verbicaro, Rodrigues e Ataíde (2018, p. 181):

> Essa considerável relevância atribuída aos bens resultou em uma supervalorização da opinião alheia acerca de símbolos de consumo e modo de vida que se adota. Ou seja, o consumidor já não se preocupa apenas em comprar o que lhe parece útil ou aprazível, mas também com o que seu conjunto de bens pode dizer sobre os traços da personalidade que deseja mostrar.

Verbicaro e Caçapietra (2021), ao analisarem a vulnerabilidade comportamental sob a perspectiva da economia comportamental, destacam que o consumidor não tem plena consciência dos critérios de tomada de decisão. Isso porque o *marketing* utiliza mecanismos da economia comportamental para explorar o raciocínio impulsivo – responsável por escolhas automáticas movidas por estados emocionais – e o raciocínio de cognição superficial – que concentra os comportamentos habituais e rotineiros.

Por outro lado, a teoria da autodeterminação (***self-determination theory*** (SDT)) reuniu um corpo de evidências empíricas na psicologia relacionadas à autonomia, a necessidades psicológicas e ao bem-estar social. Em seus traços mais amplos, a SDT identifica um conjunto de necessidades psicológicas básicas consideradas como essenciais para a automotivação, o controle de comportamentos e o bem-estar psicossocial. Essas necessidades básicas são: autonomia (sentir vontade e volição em ação), competência (sentir-se capaz e eficaz) e relacionamento (sentir-se conectado e envolvido) (CALVO *et al*., 2020).

As evidências identificadas pela teoria SDT facilita o uso da tecnologia e do *design* nas ações que envolvem modulação comportamental no ambiente virtual. O modelo METUX (*Motivation, Engagement and Thriving in User Experience*) apresenta seis "esferas de experiência de tecnologia" em que a tecnologia pode ter um impacto nas necessidades psicológicas: a) adoção, relacionada à experiência de uma tecnologia e de sua força persuasiva, como na indução à compra ou no encorajamento à escolha; b) interface, ligada à experiência do usuário na interação com o *software*; c) tarefa, referente a atividades discretas facilitadas pela tecnologia, d) comportamento, reunindo atividades que estimulam comportamentos gerais, como contagem de passos no estímulo ao exercício; e) vida, que identifica como a tecnologia influi na satisfação de necessidades psicológicas; f) sociedade, que envolve o impacto em toda a sociedade, inclusive naqueles que não utilizam a tecnologia (CALVO *et al.*, 2020).

Tal perspectiva confirma a tendência de explorar a reação emocional do consumidor por meio de abordagens publicitárias inspiradas em uma engenharia tecnológica. Essa engenharia

tecnológica auxilia os anunciantes a elaborarem testes estatísticos para identificar as narrativas mentais do público. Com o *Big Data*, a persuasão é mais específica em razão da captação de dados pessoais e do direcionamento publicitário (AKERLOF; SHILLER, 2016, p. 53-54). O mercado vale-se da fragilidade dos consumidores, que nem sempre sabem o que realmente querem e aquilo de que necessitam, para agir no seu inconsciente, gerando necessidades e vontades. Explorando a servidão voluntária contemporânea na tomada de decisão, o mercado faz o consumidor convencer-se de que é mais fácil seguir os ditames impostos pelo mercado do que assumir a angustiante responsabilidade por uma decisão racional.

Pode-se ainda relacionar a vulnerabilidade comportamental do consumidor com a obsolescência psicológica (SANTIAGO; ANDRADE, 2016): mecanismos de indução, de instigação, de sedução dos consumidores levam-nos a gastar reiteradamente de forma a tornar o produto obsoleto na sua psique por associarem o novo ao melhor, em oposição ao velho, ao antiquado e ao obsoleto.

Em outro sentido, Albuquerque (2014, p. 133-140) finca as raízes da vulnerabilidade psíquica na teoria do desamparo de Freud. O mundo é marcado por inseguranças, traumas e desamparo. Para o bebê, o útero da mãe é uma fonte de proteção e de amparo; no restante de sua vida, buscará o amor da mãe. Na sociedade capitalista, o consumo, como modalidade de comportamento, é equivalente à figura materna, representando uma solução de proteção contra desamparos e inseguranças. De acordo com os ditames da indústria cultural, a satisfação dos desejos será obtida pelas necessidades mercadológicas.

Quando o consumidor é excessivamente exposto às práticas persuasivas de *marketing*, deixando-se seduzir pelas promessas de felicidade e de satisfação plena por meio do consumo, sua vulnerabilidade psíquica poderá ser agravada de acordo com o contexto em que estiver inserido, "da cultura da qual tem parte e dos mecanismos [de] que a civilização se vale para impor seu poder, suas ideias e suas promessas de sedução" (ALBUQUERQUE, 2014, p. 140). Para Ataíde (2020, p. 140), a vulnerabilidade psíquica é uma característica de várias categorias de consumidores, mas o consumidor de saúde destaca-se pelo excesso de confiança na indústria farmacêutica e na literatura médica[75].

[75] "Com tantas promessas veiculadas pelos meios de comunicação de massa, que se espraiam a nível planetário, cria-se excesso de confiança nas fórmulas oferecidas no mercado global de saúde. Nessa ambiência, se não fantasiosa, mas exagerada dos benefícios proporcionados, o principal tende a ser negligenciado, que são as informações relevantes sobre efeitos colaterais, efeitos de dependência física e psicológica, as interações medicamentosas. As chances de insucesso do tratamento e o comportamento da renda com o uso habitual de certos fármacos. Ainda, o excesso de confiança no saber médico, nas prescrições e orientações dos profissionais de saúde, em especial médicos, também insere o consumidor em um acentuado estado de vulnerabilidade" (ATAÍDE, 2020, p. 140-141).

Na economia de dados, a vulnerabilidade psíquica e a vulnerabilidade comportamental do consumidor virtual estão ligadas, uma vez que a publicidade direcionada tem por objetivo explorar a irracionalidade e a compulsão do consumidor, o desejo subjetivo de pertencimento e de proteção[76] por meio do consumo. Consequentemente, a fragilidade do consumidor ante as práticas predatórias de *marketing*, o direcionamento e a subjetivação do ciberespaço influem diretamente no seu poder de escolha.

É fato que a publicidade direcionada é uma expressão do assédio de consumo por ter como finalidade convencer o consumidor a se envolver com determinado produto ou marca. A constante necessidade de pertencimento faz com que sua liberdade de escolha seja reduzida (VERBICARO; RODRIGUES; ATAÍDE, 2018).

A vulnerabilidade psicocomportamental, portanto, vincula-se ao processo de tomada de decisão. Portanto, o tratamento de dados, o direcionamento publicitário e o assédio de consumo no mercado informacional não somente estimulam comportamentos, mas também atingem o desenvolvimento subjetivo de cada consumidor, suas angústias e suas emoções, o que gera reflexos sociais pela modulação comportamental coletiva.

3.1.3 A nova dimensão da vulnerabilidade situacional do consumidor

Como estudado na subseção 3.1, a vulnerabilidade do consumidor pode ser relacional, invariável ou mutável. A mutabilidade está atrelada ao ao espaço-tempo em que cada consumidor está inserido. Assim, para determinar a vulnerabilidade situacional, é preciso examinar a situação real e a realidade do cotidiano do consumidor. Por isso, diz-se que a vulnerabilidade situacional é fluida e construída socialmente (BAKER, 2009). Xavier e Riemenschneider (2019, p. 7) afirmam:

> Há casos de vulnerabilidade acentuada que se mostram permanentes, irreversíveis ou duradouros, como a deficiência física, sensorial ou mental, a idade cronológica avançada e os portadores de doenças sujeitas a tratamentos longos. Porém, também não se pode descuidar da existência de situações de hipervulnerabilidade situacional, decorrente de determinado fator que possui limitação temporal […].

[76] Proteção no sentido de entender o consumo como uma forma de inclusão social e de satisfação emocional, o que vai além de impulsos comportamentais. Segundo Verbicaro e Caçapietra (2021, p. 7), "justamente para atender à sedução de uma falseada felicidade artificial, [...] o consumidor se vê obrigado a concentrar todos os seus esforços em tornar sua vida economicamente produtiva, seja no trabalho, seja no âmbito das relações familiares, ou mesmo na artificialidade de sua vida social, de modo a melhor otimizar seu já escasso tempo para ser bem-sucedido na satisfação das inúmeras necessidades de consumo, forjadas pela indústria cultural que, agora, serve maciçamente ao consumo".

Embora alguns consumidores apresentem uma condição de vulnerabilidade no comércio eletrônico exacerbada pelo grau de imersão tecnológica, a vulnerabilidade do consumidor no ciberespaço é situacional por se vincular ao mercado informacional.

A contratação eletrônica[77] fragiliza o equilíbrio relacional entre as partes dada a ausência informativa. Tanto na captura de dados pessoais quanto na sua utilização pela publicidade direcionada, é possível diagnosticar um "traço vulnerabilizante peculiar"[78] que influenciará o exercício da autonomia de vontade do consumidor.

Certos modelos de Inteligência Artificial vinculam-se à captura de dados. Por exemplo, a função principal do celular não é a absorção das rotas do consumidor via GPS, no entanto, não só o celular faz isso como transforma essa captação de dados em publicidade direcionada para o consumo de bens e serviços fornecidos por empresas de GPS. Pode-se destacar ainda que, mesmo que se recuse a utilização de aplicativos e de serviços coletores de dados, o acesso à rede de transmissão possibilita o acesso a dados. Nesse sentido, o contexto em que o consumidor está inserido é decisivo para a disponibilização de informações pessoais, o que caracterizado sua vulnerabilidade situacional (VERBICARO; VIEIRA, 2021a).

A vulnerabilidade situacional na economia de dados, portanto, é caracterizada pela liberdade mitigada no contexto em que o negócio está inserido. Diante das características da contratação por adesão e impossibilidade de exercício da negativa, seja em utilizar o produto e serviço ou ainda em quais dados quer dispor. Ser vulnerável situacional é ter sua liberdade relativizada pela situação em que está inserido (VERBICARO; VIEIRA, 2021a). Nesse sentido, quando se utiliza como base legal o consentimento, é necessário observar a plena concretude da autonomia de vontade do consumidor.

3.1.4 A vulnerabilidade algorítmica na assimetria de controle e informação

A condição de vulnerabilidade atinge todos os consumidores. No entanto, em razão da circunstância negocial em que o consumidor digital está envolvido, diversos tipos de vulnerabilidades são possíveis. Não se trata, porém, de determinar as subespécies do princípio da vulnerabilidade, trata-se apenas de identificar o melhor arcabouço normativo para a proteção

[77] Ver subseção 3.1.

[78] Bioni (2020a, p. 157) utiliza essa expressão para apresentar a assimetria informacional como premissa intensificadora da vulnerabilidade do consumidor. Neste trabalho, adota-se uma concepção ampliada ante a indiscutível vulnerabilidade informacional do consumidor (conforme tópico 31.1) agravada pelas características da contratação eletrônica – despersonalização, desterritorialização, desmaterialização, atemporalidade da contratação e hiperconfiança.

do consumidor, não se excluindo o que há em comum entre as (agravantes) vulnerabilidades apresentadas.

Assim, o consumidor assediado pela publicidade direcionada por meio do uso indevido de seus dados pessoais é, ao mesmo tempo, vulnerável situacional (pelo contexto em que se insere), vulnerável psicocomportamental (pelas estratégias de *marketing*) e vulnerável informacional (por não ter informações qualificadas tanto sobre a relação pré-contratual da coleta de seus dados, quanto sobre o direcionamento publicitário, e menos ainda sobre o negócio a ser contratado e/ou comprado). Poder-se-ia então falar em um controle biopolítico sobre os corpos, em que não há distinção entre o corpo físico e o virtual, realizado pelo dito *Big Other*[79]?

Com base nos ensinamentos de Foucault (1999, 2008, 2015), Deleuze (1992), Han (2018) e Zuboff (2018, 2020), acredita-se que o desequilíbrio entre as partes na economia de dados pessoais é resultado de uma assimetria de poder, de controle e de informação, o que configura vulnerabilidades algorítmicas:

> A vulnerabilidade algorítmica ou tecnoregulatória possui como núcleo distintivo a massiva coleta de dados pessoais que o consumidor é alvo no ambiente digital e o seu ulterior tratamento através de códigos de programação conhecidos como algoritmos executados pelas máquinas dos fornecedores em geral, notadamente das plataformas de mídia social (social media). Os dados dos consumidores são utilizados para se fazer uma edição invisível voltada à customização da navegação no ciberespaço. Através do tratamento de dados com algoritmos, as plataformas virtuais procedem a uma espécie de personificação dos conteúdos da rede, a partir das características de navegação e interesses daquele usuário-consumidor, coletados através de cookies ou pegadas digitais, criando para ele um microcosmo particular no ambiente virtual que condiciona os rumos de sua navegação no ciberespaço. Este procedimento restringe as possibilidades de livre navegação no ciberespaço em decorrência de filtros-bolha (filter bubble) que limitam as informações a partir daquilo que as máquinas determinam ser de interesse do usuário, tecnoregulando as suas experiências (MILHOMENS, 2021, p. 202).

Há ausência de transparência no processo de coleta, no tratamento e no uso dos dados pessoais dos consumidores, que são segmentados e, a partir disso, direcionados para a compra de determinados bens e serviços de acordo com as suas predileções. O consumidor não tem poder e controle sobre as suas informações. Há um abismo informativo em todo o ciclo mercadológico que envolve suas informações pessoais.

Para Verbicaro e Vieira (2021a, p.205), a vulnerabilidade algorítmica é decorrente da "captação, tratamento e difusão indevidos dos dados pessoais do consumidor, às vezes por intermédio de dispositivos dotados de inteligência artificial, em franca violação aos direitos da personalidade, como a privacidade e intimidade". Para os autores, tal vulnerabilidade é consequência de hiperconfiança do consumidor no consumo digital, da insuficiência

[79] Ver Capítulo 2.

tecnonormativa, do abstencionismo estatal e do protagonismo das grandes plataformas virtuais (VERBICARO, VIEIRA, 2021a, p. 205).

Constata-se, portanto, que os direitos fundamentais da privacidade, da igualdade e da liberdade ficam fragilizado pelos seguintes motivos: a) contrair a direito negativo quanto à preservação de seus dados pessoais; b) não há equidade entre os atores da relação, em razão do direcionamento pelo mercado de escolhas e comportamentos dos consumidores em benefício de fornecedores, bem como do protagonismo de grandes plataformas virtuais; c) não existe autonomia de vontade e controle informacional por causa da modulação algorítmica de dados pessoais.

3.2 Privacidade: um conceito multiforme

A privacidade está ligada à percepção social do indivíduo. As raízes do direito à privacidade estão na emergência do Estado-nação e da sociedade civil nos séculos XVI e XVII, bem como no estabelecimento da esfera privada livre das ingerências do ente público como, inclusive, reação ao absolutismo (DONEDA, 2019, p. 118). Cabe ainda citar o fortalecimento da burguesia e do individualismo que contribuiram para o desenvolvimento da ideia moderna de privacidade.

Privacidade é um conceito aberto, vago. Dependendo do doutrinador, será abrangente ou restritivo (LEONARDI, 2012, p. 48):

> Assuntos como liberdade de pensamento, controle sobre o próprio corpo, quietude do lar, recato, controle sobre informações pessoais, proteção da reputação, proteção contra buscas e investigações, desenvolvimento da personalidade, autodeterminação informativa, entre outros, são excluídos ou incluídos, de acordo com a definição adotada.

Doneda (2019, p. 101) destaca que a dificuldade reside não na definição de privacidade, mas no que se espera dessa definição. O contexto no qual se busca definir a privacidade é reduzido “a uma perspectiva epistemológica conceitualística, que visa (por vezes sem consciência), em primeiro lugar, à coesão do sistema, operando precisamente através de um processo de generalização do qual a individualização de um conceito dogmático é seu ápice ” (DONEDA, 2019, p. 100).

Leonardi (2012, p. 48-51) afirma ainda que a delimitação de um conceito único é difícil em diversos países[80]. No entanto, as tentativas de conceituação de privacidade seguem o método

[80] “Importante observar que o problema não se reduz a uma dicotomia entre o modelo da Civil Law e o da Common Law: ainda que existam diferenças substanciais entre o modelo de privacidade romano-germânico (que adota como principal fundamento a dignidade) e o modelo de privacidade anglo-saxão (que adota como principal

per genus proximum et differentiam – pelo gênero próximo e pela diferença específica. Os atributos principais do princípio da exclusividade que rege a privacidade são: a) o direito de estar só (*right to be alone*), b) o resguardo contra interferências de terceiros, c) o sigilo e d) o controle sobre dados pessoais. Para Doneda (2019, p. 129), a privacidade é um conjunto de valores e situações pautadas por uma lógica subjetiva. Daí o seu caráter relacional por estar além da sua função patrimonial relacionada ao raciocínio de "espaços" ou "bens" a serem protegidos, mas sob o viés de administração das escolhas.

A primeira menção à privacidade remete à proteção sagrada da vida doméstica privada. Warren e Brandeis (1890) são os precursores do direito de estar só, na sua essencialidade individualista. A inviolabilidade da personalidade, de caráter negativo, traduzir-se-ia no dever de abstenção por parte de terceiros contra invasões dos "limites óbvios da decência e da propriedade" (WARREN; BRANDEIS, 1890, p. 196, tradução nossa). Sua subjetividade intrínseca está ligada a dimensão da proteção da privacidade, ligando-se ao desenvolvimento social, político e econômico e está relacionada à individualidade de cada um, sua honra, sua propriedade e sua dignidade – o direito de estar só (*right to be alone*).

Warren e Brandeis (1890), em seu artigo *The Right to Privacy*, foram os primeiros a definir o conceito de *privacy*, desvinculando-o da propriedade privada e associando-o à inviolabilidade da personalidade, sendo a vida privada objeto de tutela. Tal artigo deve ser entendido como um marco das discussões sobre privacidade:

> (i) partia-se de um novo fato social, que eram as mudanças trazidas para a sociedade pelas tecnologias (jornais, fotografias) e a comunicação de massa, fenômeno que se renova e continua moldando a sociedade futura; (ii) o novo "direito à privacidade" era de natureza pessoal, e não se aproveitava da estrutura da tutela da propriedade para proteger aspectos da privacidade; (iii) no que interessa somente aos EUA, o artigo abriu o caminho para o reconhecimento (que ainda tardaria décadas) do direito à privacidade como um direito constitucionalmente garantido (DONEDA, 2019, p. 126).

Quanto à concepção de privacidade como resguardo contra interferências alheias, conforme a definição proposta na Conferência Nórdica sobre o Direito à Intimidade, realizada em 1967, trata-se do direito de viver com um grau de interferência mínima de terceiros, o que também é de caráter negativo. Para Leonardi (2012, p. 56), isso "representa o direito de o indivíduo manter seus assuntos para si e decidir por si mesmo em que medida eles serão submetidos à observação e discussões públicas". Segundo Bittar (1994, p. 273-278), aborda o

---

fundamento a liberdade), não se pode perder de vista que, mesmo entre os sistemas de Common Law do Reino Unido e dos Estados Unidos, há diferenças significativas entre o âmbito de proteção do direito à privacidade. Além disso, ainda que o direito europeu caminhe, por meio de diversas diretivas relacionadas à privacidade, para uma uniformização relativa – ao menos no que tange aos padrões mínimos de proteção – há importantes diferenças culturais entre países-membros da União Europeia, as quais influenciam, por óbvio, a transposição desses padrões mínimos no direito interno de cada nação" (LEONARDI, 2012, p. 49-50).

isolamento mental necessário para resguardar certos aspectos subjetivos da vida privada contra terceiros, ressaltando-se o direito à intimidade e ao segredo[81]. Em seu voto no Mandado de Segurança 23.669-DF, o Relator, Ministro Celso de Mello, da 2.ª Turma do STF, assim se manifestou:

> O direito à intimidade – que representa importante manifestação dos direitos da personalidade – qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada. A transposição arbitrária, para o domínio público, de questões meramente pessoais, sem qualquer reflexo no plano dos interesses sociais, tem o significado de grave transgressão ao postulado constitucional que protege o direito à intimidade, pois este, na abrangência de seu alcance, representa o "direito de excluir, do conhecimento de terceiros, aquilo que diz respeito ao modo de ser da vida privada"[82].

Há crítica ao conceito de privacidade no que diz respeito ao resguardo contra interferências alheias por entender pela ausência de delimitação específica da interferência uma vez que defende que nem toda interferência poderá ser considerada intromissão. Assim, o conceito de privacidade não apresenta parâmetros claros e limites bem definidos (LEONARDI, 2012, p. 61).

A privacidade, ao ser definida como sigilo, apresenta um *status* duplo – público e privado –, uma vez que será estabelecida a violação da privacidade quando houver revelação pública de informação pessoal, antes mantida em sigilo[83]. Não se pode equiparar a ideia de segredo a sigilo absoluto porque se deve considerar a relativização e o desejo de confiabilidade de exposição a determinados grupos e pessoas (LEONARDI, 2012, p. 62-66). Nesse sentido, o direito ao sigilo é a liberdade de não emitir pensamentos para todos, é o exercício de poder de escolher quais pessoas receberão suas ideias e manifestações.

Por outro lado, Rodotà (2008) afirma que o desenvolvimento da tecnologia abarcou novas realidades com difusão interativa e perspectivas abertas de telemática. A tecnologia

---

[81] Bittar (1989) apresenta uma tríplice classificação dos direitos da personalidade, que seriam físicos, psíquicos e morais. O autor insere nos direitos psíquicos a intimidade (estar só, privacidade ou reserva) e o segredo (ou sigilo, inclusive profissional). Ver ainda Marcacini (2019, p. 133).

[82] STF (2. Turma). Mandado de Segurança 23.669/DF. Relator: Min. Celso de Mello. Data de julgamento: 08/02/2001. Data de publicação: DJ, 12/02/2001, p. 00017.

[83] STF (Plenário). Recurso Extraordinário 1.055.941/SP. Relator: Min. Dias Toffoli. Data de julgamento: 04/12/2019: "O Tribunal, por maioria, aderindo à proposta formulada pelo Ministro Alexandre de Moraes, fixou a seguinte tese de repercussão geral: '1. É constitucional o compartilhamento dos relatórios de inteligência financeira da UIF e da íntegra do procedimento fiscalizatório da Receita Federal do Brasil, que define o lançamento do tributo, com os órgãos de persecução penal para fins criminais, sem a obrigatoriedade de prévia autorização judicial, devendo ser resguardado o sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional. 2. O compartilhamento pela UIF e pela RFB, referente ao item anterior, deve ser feito unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios'".

reformulou não apenas o cenário tecnológico, mas também o ambiente político-jurídico-institucional, o que implicou a necessidade de ampliar a noção de privacidade no que diz respeito à proteção de dados pessoais. Assim, a noção de privacidade assumiu "contornos difusos e permeados por variadas apreciações quando foi associada à dignidade da pessoa diante das novas tecnologias" (PODESTÁ, 2019, p. 93). A esfera pessoal e a esfera pública unem-se, devendo o grau de proteção individual na esfera privada depender necessariamente do sistema político. Isso significa que as regras de circulação de informações estão destinadas a atingir a distribuição de poder na sociedade:

> Estamos diante da possibilidade de um controle social cada vez mais amplo e difuso, exercido pelos centros de poder públicos e privados. Este controle, em relação aos indivíduos, pode assentar obstáculos reais ao livre desenvolvimento da personalidade individual, imobilizado em torno de perfis historicamente determinados. E, em seu perfil sócio-político, ao privilegiar os comportamentos conformes, o controle pode tornar mais difícil a produção de novas identidades coletivas, reduzindo assim a capacidade total de inovação dentro do sistema (RODOTÀ, 2008, p. 83).

Segundo Rodotà (2008), a proteção da privacidade não está relacionada apenas ao exercício de direitos negativos, como o direito de estar só. Graças a uma reestruturação, sua proteção está ligada ao exercício da cidadania: a proteção da privacidade, nesse aspecto, está diretamente ligada ao combate de práticas de controle. Os direitos negativos de estar só, ao segredo ou sigilo, portanto, foram acrescidos pelo direito positivo de controle das informações e de seus limites na esfera privada.

Trata-se do eixo "pessoa-informação-circulação-controle", em que a proteção dos dados pessoais torna-se o elemento principal para o livre desenvolvimento da personalidade e a autonomia de vontade. Assim, privacidade consiste não apenas nos elementos subjetivos de cada um – *right to be alone* –, mas também na redistribuição de poderes sociais e legais – *right to democracy* –, "identificando-se, sem maiores entraves, o caráter democrático de um sistema com a quota de informações relevantes que circulam no seu interior" (RODOTÀ, 2008, p. 45).

Nesse sentido, o direito à privacidade está relacionado à proteção de espaços e bens, mas também à administração das escolhas pessoais no sentido de projetar a personalidade no exterior. Como consequência, assume um caráter relacional. Logo, o direito à privacidade apresenta uma dupla projeção ao ser considerado um direito fundamental e um direito da personalidade. Tal caracterização é essencial para a análise da possível autolimitação do seu exercício[84] em atenção aos conflitos de direitos. Cumpre lembrar que a privacidade foi reconhecida como direito fundamental por convenções internacionais de direitos humanos

[84] De acordo com Enunciado n.º 139 das Jornadas de Direito Civil, "Os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas em lei, não podendo ser exercidos com abuso de direito de seu titular, contrariamente à boa-fé objetiva e aos bons costumes".

ratificadas pelo Brasil·(LEONARDI, 2012, p. 95), sendo tal reconhecimento necessário nas limitações de seu exercício em caso de conflito entre direitos da mesma categoria.

A privacidade está relacionada com a capacidade individual de controlar suas informações e seus dados pessoais. Rodotà (2008, p. 93) aponta duas tendências claras na delimitação do conceito de privacidade: o poder de exclusão e a atribuição de relevante poder de controle.

Os Estados Unidos (EUA) divulgaram o relatório *Records, computers and the rights of citizens,* sugerindo cinco condutas consideradas na proteção de dados pessoais[85]:

> • Não deve existir sistema de manutenção de dados pessoais secretos.
> • Os usuários devem saber quais informações sobre eles são registradas e como são usadas.
> • Deve haver meios para o usuário impedir a utilização de seus dados com finalidade diversa da qual foi consentida;
> • Usuários devem dispor de meios para evitar que informações obtidas sobre eles para um determinado propósito sejam usadas ou disponibilizadas para outros fins sem seu consentimento.
> • Usuários devem dispor de meios para corrigir ou alterar o registro de dados pessoais.
> • Toda organização que crie, mantenha, use ou divulgue registros de dados pessoais identificáveis deve garantir o uso legítimo desses dados, tomando precauções contra seu uso indevido (U.S. DEPARTMENT OF HEALTH, EDUCATION & WELFARE, 1973, p. xx-xxi, tradução nossa)[86].

Afirma Leonardi (2012, p. 73):

> Dados armazenados em papel, ainda que públicos sejam difíceis de pesquisar e correlacionar; dados computadorizados podem ser pesquisados facilmente, e dados em rede podem ser pesquisados remotamente e correlacionados com outros dados. A novidade não é que os dados estão publicamente disponíveis, mas sim a facilidade com que podem ser coletados, usados e abusados.

O foco não deve ser restrito ao controle de informações e dados, deve alcançar o direito de tomar decisões sobre a vida, ou seja, o estabelecimento da autodeterminação informativa (LEONARDI, 2012, p. 74). Assim, a definição de privacidade em sua perspectiva de controle é abrangente e, ao mesmo tempo, restritiva. A privacidade deve, então, ser entendida como um

---

85 O relatório ainda orienta a elaboração de códigos com práticas justas: "The Code should define 'fair information practice' as adherence to specified safeguard requirements. The Code should prohibit violation of any safeguard requirement as an 'unfair information practice'. The Code should provide that an unfair information practice be subject to both civil and criminal penalties. The Code should provide for injunctions to prevent violation of any safeguard requirement. The Code should give individuals the right to bring suits for unfair information practices to recover actual, liquidated, and punitive damages, in individual or class actions. It should also provide for recovery of reasonable attorneys' fees and other costs of litigation incurred by individuals who bring successful suits" (U.S. DEPARTMENT OF HEALTH, EDUCATION & WELFARE, 1973, p. xxiii).

86 No original: "There must be no personal data record-keeping systems whose very existence is secret. There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. There must be a way for an individual to correct or amend a record of identifiable information about him. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data".

conceito plural e multiforme, para abarcar as diversas concepções, seja no sentido individual, seja no sentido coletivo[87].

É, portanto, consenso doutrinário e jurisprudencial a necessidade de uma tutela mais ampla, ante a caracterização da privacidade como direito de personalidade e como direito fundamental. Leonardi (2012, p.80-82) aduz que a CF estabelece a privacidade de modo abrangente, englobando os aspectos supracitados, ressaltando que os termos, ainda que não sejam todos sinônimos, devem ter a mesma significação e o mesmo alcance diante da fluidez, da vaguidade e da subjetividade:

> Avaliando a trajetória da matéria nas últimas décadas, revelam-se uma série de interesses a ela relacionada, não somente atinentes à reserva e ao isolamento, porém também à construção de uma esfera pessoal na qual seja possível a liberdade de escolha e, consequentemente, o desenvolvimento da personalidade (DONEDA, 2019, p. 130).

Para Marques e Miragem (2012), o direito privado sofreu uma intervenção do Estado, passando a ser orientado pelo sistema de valores constitucionais. Os direitos da personalidade, no mesmo sentido, não se exaurem nas situações previstas no Código Civil (CC). Rodotà (2008, p. 98) afirma que a possibilidade de controlar as próprias informações contribui para manter a condição do indivíduo em sociedade, sendo instrumento da tutela da personalidade pela consolidação de direitos como o *right publicity* e o direito à identidade pessoal. Trata-se de "uma tutela dinâmica e aberta para abraçar novas situações como um ferramental para promoção da pessoa humana" (BIONI, 2020a, p. 53).

A personalidade, como um conjunto de características específicas que distinguem cada um individualmente, é uma série de atributos que projetam a pessoa. Os direitos da personalidade são "inerentes à própria pessoa humana e constituem prerrogativas ou faculdades que permitem a cada ser humano o desenvolvimento de suas aptidões e energias tanto físicas como espirituais" (MATTIA, 2010, p. 5).

A proteção dos dados pessoais deve ser inserida, dessa maneira, nos direitos da personalidade porque projetam, por meio de informações específicas, o seu titular (BIONI, 2020a; DONEDA, 2019), bem como deve ser entendida como um direito fundamental (subseção 3.2.1). A proteção da privacidade, sob a perspectiva dos dados pessoais, é a garantia do exercício da autonomia de vontade e, em caráter coletivo, o exercício da democracia deliberativa.

---

[87] Leonardi (2012, p. 79) destaca que conceitos reducionistas definem a privacidade de modo limitado por isolar apenas um aspecto de sua complexa multiplicidade.

A multiformidade conceitual da privacidade pode ser verificada nas descrições legislativas do direito brasileiro. Na CF/1988, há referência à intimidade (art. 5.º, X)[88], à proteção ao domicílio (art. 5.º, XI)[89], ao sigilo de comunicação (art. 5.º, XII)[90] e ao direito ao *habeas data* (art. 5.º, LXXII)[91]. Há menção à privacidade também no artigo 43 do CDC/1990[92], no artigo 21 do CC/2002[93], na Lei n.º 12.414/2011 (Lei do Cadastro Positivo), na Lei n.º 12.527/2011 (Lei do Acesso à Informação Pública), no artigo 8.º do Decreto n.º 6135/2007[94], no artigo 11 do Decreto n.º 6.523/2008[95], no artigo 6.º do Decreto n.º 6.425/2008[96], entre outros.

---

[88] Artigo 5.º, X: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

[89] Artigo 5.º, XI: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial".

[90] Artigo 5.º, XII: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[91] Artigo 5.º, LXXII: "conceder-se-á *habeas data*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

[92] "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1.º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2.º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3.º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4.º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5.º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6.º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor".

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

[94] "Art.8.º-Os dados de identificação das famílias do CadÚnico são sigilosos e somente poderão ser utilizados para as seguintes finalidades: I - formulação e gestão de políticas públicas; e II - realização de estudos e pesquisas. § 1.º-São vedadas a cessão e a utilização dos dados do CadÚnico com o objetivo de contatar as famílias para qualquer outro fim que não aqueles indicados neste artigo. § 2.º A União, os Estados, os Municípios e o Distrito Federal poderão utilizar suas respectivas bases para formulação e gestão de políticas públicas no âmbito de sua jurisdição. § 3.º O Ministério do Desenvolvimento Social e Combate à Fome poderá ceder a base de dados nacional do CadÚnico para sua utilização, por órgãos do Poder Executivo Federal, em políticas públicas que não tenham o CadÚnico como instrumento de seleção de beneficiários. § 4.º Os dados a que se refere este artigo somente poderão ser cedidos a terceiros, para as finalidades mencionadas no *caput*, pelos órgãos gestores do CadÚnico no âmbito da União, do Distrito Federal e dos Municípios. § 5.º A utilização dos dados a que se refere o *caput* será pautada pelo respeito à dignidade do cidadão e à sua privacidade. § 6.º A utilização indevida dos dados disponibilizados acarretará a aplicação de sanção civil e penal na forma da lei".

[95] "Art. 11 Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento".

[96] "Art. 6.º Ficam assegurados o sigilo e a proteção de dados pessoais apurados no censo da educação, vedada a sua utilização para fins estranhos aos previstos na legislação educacional aplicável".

Todos os sentidos podem ser caracterizados como “círculo da privacidade” (MARCACINI, 2019, p. 134).

Mendes (2019, p. 140), ao analisar os principais julgados sobre privacidade no direito brasileiro, concluiu:

> a) As modificações sociais e tecnológicas ensejam o desenvolvimento de um novo direito à privacidade no ordenamento jurídico brasileiro, consubstanciado no direito de controle das próprias informações pessoais e no consentimento do seu titular; b) O direito fundamental à intimidade e à vida privada, previsto no art. 5, X, da CF/88, protege a esfera privada do indivíduo em diversas dimensões, inclusive na dimensão da privacidade dos seus dados pessoais e da autodeterminação de suas informações; c) Uma interpretação conjunta do art. 5, X e LXXII, da CF/88, permite, portanto, falar-se em um direito fundamental à proteção de dados pessoais no ordenamento jurídico brasileiro; d) O direito fundamental à proteção dos dados pessoais opera até mesmo nas situações em que não há sigilo dos dados, pois, como os dados se referem à personificação do cidadão, estão sob a sua esfera de autonomia; e) Nas relações de consumo, há um generalizado processamento de dados pessoais ampliando-se os riscos à personalidade dos consumidores; f) O Código de Defesa do Consumidor, em seu art. 43 e em seus princípios, estabelece a proteção à personalidade e à privacidade do consumidor, também na sua dimensão da proteção de dados pessoais; g) A utilização dos dados pessoais do consumidor em contexto diverso daquele que já foi autorizado fere o princípio da finalidade e enseja a violação da privacidade do consumidor; h) O abuso da empresa em relação à utilização dos dados pessoais do consumidor ou a omissão em instituir sistemas de proteção da privacidade (princípio do risco da atividade) caracteriza danos morais e enseja o dever de indenizar.

As múltiplas perspectivas da privacidade, portanto, vão além de um valor em si. Na verdade, trata-se de uma forma de proteção da pessoa humana que se insere no controle das informações, como em situações existenciais (DONEDA, 2019, p. 132), englobando concepções patrimoniais, não patrimoniais, negativas e positivas.

3.2.1 A proteção dos dados pessoais como direito autônomo e fundamental

Dado tem uma conotação fragmentada e primitiva. É o estado inicial, ensejador da informação. Já a informação[97] está além da representação contida no dado, pressupõe a depuração do conteúdo no limiar cognitivo (DONEDA, 2019, p. 136). No que diz respeito à caracterização de informações pessoais, é importante frisar o vínculo objetivo no seu tratamento por relacionar as suas especificidades e atribuições pessoais, sendo, nesse sentido, indissolúvel da pessoa em referência. Nesse sentido, o corpo virtual e o corpo físico entrelaçam-se e são representados por essas informações pessoais em circulação na internet.

[97] As informações são classificadas em quatro modalidades: relativas a pessoas e patrimônios, opiões pessoais, obras do espírito e descrições de fenômenos, coisas e eventos (CATALA, 1983, p. 22; DONEDA, 2019, p. 139).

O dado pode dizer respeito a uma pessoa específica ou a uma pessoa indeterminada, de acordo com o grau de (pseudo)anonimização. O banco de dados é um conjunto de informações organizadas por meio de uma lógica estrutural e tecnológica. A noção de banco de dados amplia-se e se desenvolve com o avanço tecnológico. No entanto, não é apenas esse contexto que determina a necessidade de reestruturação do conceito de privacidade. A modificação do ambiente jurídico-institucional é fator imperioso para o desenvolvimento de uma noção "mais completa" da tutela de dados pessoais (RODOTÀ, 2008, p. 44).

Para Doneda (2019, p. 141), a concepção do banco de dados deixou de ser central diante da necessidade de proteção da informação pessoal ampla, relacionada não mais apenas aos grandes repositórios, mas agora às técnicas individuais de coleta, de agregação e de uso de dados pessoais, inclusive os sensíveis.

Os dados sensíveis são ainda mais específicos, e seu uso indiscriminado pode ter maior grau de potencial lesivo ao consumidor. Isso porque são relacionados a determinadas informações específicas do titular e de sua esfera íntima. Segundo Carvalho (2003, p. 8), a doutrina classifica os dados da seguinte forma:

> a) públicos, que importam a toda a sociedade, atendendo a sua divulgação ao direito de informar e de ser informado, tais como informações sobre acidentes e crimes, sobre as eleições, os gastos públicos, a higidez do mercado e das relações de consumo etc.; b) pessoais de interesse público, como o nome, o domicílio, o estado civil, a filiação, o número de identificação do indivíduo; c) sensíveis, que dizem respeito à esfera íntima do indivíduo, como os seus pensamentos, as suas opiniões políticas, a sua situação econômica, a sua raça, a sua religião, a sua vida conjugal e sexual, e outras condições que importam apenas ao indivíduo.

Com a revolução tecnológica, a privacidade desvinculou-se de seu sentido individualista, negativo e privado para ser divisível, para possibilitar que cada um decida se suas informações podem ser disponibilizadas, como visto na subseção anterior. Indo além das relações privadas, a privacidade agora diz respeito ao exercício político-democrático que permite a cada indivíduo expressar suas decisões, vontades e características. A problemática da coleta de informações altera, porém, a noção da privacidade como exercício de controle individual e coletivo:

> Parece claro que esse processo de revisão hoje é diretamente condicionado pela avançada transformação do sistema informativo em seu conjunto, da qual o tratamento de informações através computadores constitui somente uma parte. A caracterização da nossa organização social como uma sociedade cada vez mais baseada sobre a acumulação e a circulação de informações comporta o nascimento de um novo e verdadeiro "recurso" de base, ao qual se coliga o estabelecimento de novas situações de poder (RODOTÀ, 2008, p. 35).

Nesse sentido, a privacidade desliga-se do seu tradicional quadro individualista e dilata-se em uma dimensão coletiva, sendo considerado não apenas o interesse individual, mas

também o grupo ao qual o indivíduo pertence (RODOTÀ, 2008, p. 30). Assim, não se pode privilegiar um contexto especial de proteção, é preciso adotar estratégias integradas, capazes de regular a circulação de informações em seu conjunto (RODOTÀ, 2008, p. 50). Nesse aspecto, diretrizes relativas à proteção da vida privada e à circulação transnacional de dados de caráter pessoal são fundadas em premissas basilares: correção, exatidão, finalidade (pertinência, utilização não abusiva e direito ao esquecimento), publicidade, acesso individual e segurança (RODOTÀ, 2008, p. 59).

Além de uma tutela mais intensa e do sigilo de informações relevantes, a proteção da privacidade precisa garantir a cada indivíduo a possibilidade de conhecer e de controlar suas informações. O princípio do *control of information about oneself* representa o poder autônomo de controle[98] e o direito de acesso é primordial no exercício do direito fundamental de proteção dos dados pessoais:

> O reconhecimento da condição de direito fundamental à privacidade, do ponto de vista de poder "acompanhar" as informações pessoais mesmo quando se tornaram objeto de disponibilidade de outro sujeito, deu relevo especial ao direito de acesso, que se tornou a regra básica para regular as relações entre sujeitos potencialmente em conflito, superando o critério formal da posse das informações (RODOTÀ, 2008, p. 97).

As leis de proteção de dados pessoais podem ser divididas em gerações: na década de 70 do século XX, em razão do fenômeno computacional, havia a convicção de que liberdades e direitos estariam ameaçados pela coleta de dados realizada pelo Estado; depois, passou-se à proteção da liberdade negativa do cidadão pelo processamento de dados por terceiros; na década de 80, essa proteção englobava a efetividade da liberdade em sentido amplo – o exercício da autodeterminação informativa; finalmente, chegou-se ao reconhecimento do desequilíbrio da relação e, conforme o contexto do tratamento de dados, à redução da autodeterminação informativa pelo fato do alto grau de complexidade tecnológica não admitir a simples decisão individual de forma racional e consciente (DONEDA, 2019, p. 174-179).

Mendes (2019, p. 170-171) destaca que, de acordo com a experiência normativa e institucional brasileira relacionada à proteção de dados pessoais, é possível reconhecer um direito fundamental à proteção de dados pessoais, como dimensão da inviolabilidade da intimidade e da vida privada[99]. Doneda (2019, p. 105) constata a ausência de uma determinação

---

[98] O exercício de controle do acesso às informações sobre si mesmo é do âmbito da "privacidade informacional". Essa concepção de privacidade em um sentido normativo "refers typically to a non-absolute moral right of persons to have direct or indirect control over access to (1) information about oneself, (2) situations in which others could acquire information about oneself, and (3) technology that can be used to generate, process or disseminate information about oneself" (VAN DEN HOVEN *et al*., 2020).

[99] A autora relaciona essa dimensão à proteção de dados pessoais descrita na Convenção 108 do Conselho da Europa e na Diretiva Europeia 95/46/CE (MENDES, 2019, p. 171-172).

terminológica clara da doutrina e da jurisprudência, bem como a necessidade de uma discussão dogmática dos limites conceituais diante de seu alto grau de subjetividade.

Ainda, a proteção de dados pessoais deve ser entendida num sentido duplo: visa proteger a integridade moral da pessoa, componente da dignidade da pessoa humana, e a liberdade no sentido amplo:

> O âmbito da proteção do direito fundamental à proteção de dados pessoais pode ser concebido em uma dupla dimensão: ele consiste, ao mesmo tempo, (i) na proteção do indivíduo contra riscos que ameaçam a personalidade em face da coleta, processamento, utilização e circulação de dados pessoais e (ii) na atribuição ao indivíduo da garantia de controlar o fluxo de seus dados na sociedade (MENDES, 2019, p. 176).

A proteção de dados pessoais engloba, portanto, o direito negativo de não intervenção estatal, segundo o qual somente o titular deverá determinar a extensão do controle e da circulação dos seus dados pessoais, sem esquecer que tal atribuição não é absoluta. O poder de controle também se manifesta na esfera negativa (RODOTÀ, 2008, p. 109).

Ademais, é mister frisar a importância do estabelecimento de garantias de exercício dos direitos de transparência, finalidade, acesso, retificação, cancelamento, entre outros, para efetivação da proteção de dados pessoais e, consequentemente, para garantir o direito à autodeterminação informativa, conforme será analisado na subseção 3.2.2. Para isso, o Estado deve estabelecer uma arquitetura institucional adequada para garantir a efetividade dessa proteção[100].

É importante destacar a possibilidade de compartilhamento de dados pessoais admitido pela MP 954/2020, o que ensejou a propositura da ADI 6387 pela violação de direitos fundamentais, especialmente da dignidade da pessoa humana, da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, do sigilo dos dados e da autodeterminação informativa, dispostos nos artigos 1.º, III, e 5.º, X e XII, da CF.

Assim, em 24 de abril de 2020, em medida cautelar por decisão monocrática, a Ministra Rosa Weber determinou a suspensão da MP 954 por entender pela ausência de transparência, finalidade, adequação e proporcionalidade das medidas de compartilhamento de dados admitidas pela Lei, além do desrespeito à autodeterminação informativa e ao direito à privacidade, necessários na análise de qualquer estratégia que envolva dados pessoais, em atenção aos direitos fundamentais e princípios estabelecidos na LGPD. Em 6 e 7 de maio de

[100] Mendes (2019, p. 181) afirma que o Estado deve garantir uma arquitetura institucional contra os riscos decorrentes do processamento de dados pelo setor público privado. No setor público, o Legislativo deve adequar e formular leis protetivas; o Judiciário deve tomar decisões ante a ausência e a insuficiência do legislador; o Executivo detém toda a estrutura administrativa e de controle.

2020, a decisão monocrática foi confirmada pela Corte do STF, que reconheceu a proteção dos dados pessoais como direito fundamental autônomo[101].

Para Mendes (2020), a decisão é um marco histórico para a proteção dos dados pessoais por reconhecer a proteção de dados pessoais como direito fundamental, impor deveres negativos e positivos ao Estado quanto a sua proteção e indicar que a prorrogação da LGPD e a ausência da ANPD são claras contrariedades aos parâmetros constitucionais. É inegável, portanto, a controvérsia estabelecida sobre a definição do conceito de privacidade. Por outro lado, há a decisão histórica e o reconhecimento da proteção dos dados pessoais como direito

[101] "MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA N.º 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2.º, I e II, da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5.º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5.º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam 'adequados, relevantes e não excessivos em relação a esse propósito' e 'conservados apenas pelo tempo necessário' (artigo 45, § 2.º, alíneas "b" e "d"). 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória n.º 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n.º 954/2020 desatende a garantia do devido processo legal (art. 5.º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP n.º 954/2000 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP n.º 954/2020. 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocados como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória n.º 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada" (STF (Tribunal Pleno). ADI 6387/DF. Relatora: Min. Rosa Weber. Data de julgamento: 07/05/2020. Data de publicação: 12/11/2020).

fundamental autônomo, considerando-se ainda o direito à autodeterminação informativa, a ser desenvolvido a seguir.

3.2.2 A autodeterminação informativa

A autodeterminação informativa significa, de modo geral, o poder de controlar suas próprias informações. Alan Westin, na sua obra *Privacy and Freedom*, publicada em 1967, já utilizava o termo para designar o direito que os indivíduos têm de decidir sobre suas próprias informações. Neste trabalho, focam-se as discussões travadas na Corte Alemã no julgamento contra a lei que organizava o censo – Volkszählungsgesetz[102]. A sentença da *Bundesverfassungsgericht* é referência por definir critérios principiológicos para o uso dos dados pessoais e examinar a autodeterminação informativa no contexto de tratamento de dados (WESTIN, 1967).

A Corte suspendeu o censo e declarou inconstitucionais os artigos da Lei em discussão por contrariarem o direito da personalidade, especialmente pela inobservância do princípio da finalidade – a Lei definia que os dados pessoais coletados poderiam ser utilizados para o censo e por órgãos administrativos para identificação dos titulares –, pela desmistificação da afirmação de que certos tipos de tratamento de dados são irrelevantes, mesmo anonimizados, dada a possibilidade de identificação do titular por meio de engenharia reversa, e pela utilização da expressão autodeterminação informativa para designar a possibilidade que cada um tem de decidir sobre os limites da utilização de seus dados pessoais (DONEDA, 2019, p. 167-168). Tal direito não é, porém, absoluto, a limitação da autodeterminação informativa ocorrerá em razão de interesse geral predominante previsto em lei em conformidade com a Constituição Federal (MENDES, 2019, p. 188).

Atualmente, a doutrina alemã critica a utilização do conceito da autodeterminação ligado exclusivamente à proteção da personalidade. Há um consenso doutrinário segundo o qual a proteção de dados pessoais tem duas dimensões: uma dimensão subjetiva (*innere Entfaltungsfreiheit*), que diz respeito à proteção da integridade moral e da personalidade, ao livre desenvolvimento do indivíduo, e uma dimensão exterior (*außefere Entfaltungsfreiheit*,

[102] A Lei do Censo estabelecia que cada cidadão deveria responder a 160 perguntas. Alguns pontos eram controversos: a possibilidade de confrontação de dados com o registro civil para retificação; a transmissão às autoridades e a existência de multa pecuniária elevada em caso da negativa de respostas e de mecanismos de favorecimento de pessoas que denunciassem aqueles que não tivessem respondido na integralidade (DONEDA, 2019, p. 165-166).

relacionada à proteção do direito geral à liberdade e das liberdades específicas (MENDES, 2019, p. 175).

Para Mendes (2019, p. 176), o reconhecimento dessa dupla dimensão é o entendimento mais apropriado: a proteção dos dados pessoais, garantindo o direito à autodeterminação informativa, influencia os direitos fundamentais na sua integralidade por proteger contra os riscos que ameaçam a personalidade, inerentes à coleta, ao tratamento e ao uso dos dados pessoais, e por assegurar o controle do fluxo dos dados pessoais.

No mesmo sentido, Ferraço (2019, p. 9) afirma que a autodeterminação informativa relaciona-se às "informações que podem ser coletadas, assim como ao poder escolher o que pode ser revelado, o que deve ser esquecido, elementos tais que dizem respeito à esfera íntima constituinte da personalidade da pessoa humana".

No sistema normativo, a Directiva Europeia de Proteção de Dados Pessoais n.º 95/46/EC[103] e a Regulação de Proteção de Dados no Direito Comunitário Europeu (*General Data Protection Regulation*)[104] têm a autodeterminação informativa como premissa basilar para o tratamento de dados pessoais. No mesmo sentido, a LGPD – Lei n.º 13.709/2018 – e o PL 3514/2015[105] têm como fundamento a autodeterminação informativa e a privacidade[106]. Especialmente, a LGPD ressalta, em diversos artigos[107], a necessidade do consentimento ativo como uma das hipóteses autorizadoras ante os direitos básicos dos titulares, particularmente o direito de acesso, de retificação, de oposição e de cancelamento, em harmonia com o CDC, que estabelece, em seu artigo 43, como direitos basilares a transparência, a comunicação e o acesso.

[103] Ver artigos 2.º, 7.º e 8.º da Directiva Europeia de Proteção de Dados Pessoais nº 95/46/EC (UNIÃO EUROPEIA, 1995).

[104] Ver artigo 4.º da Regulação de Proteção de Dados no Direito Comunitário Europeu (*General Data Protection Regulation*) (UNIÃO EUROPEIA, 2018).

[105] O PL 3514/2015 tem como objeto a alteração do CDC para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico. Encontra-se, atualmente, na Mesa Diretiva da Câmara dos Deputados.

[106] LGPD: "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".

[107] Ver artigos 5.º, XII, 7.º, I, § 4.º, § 5.º, § 6.º, 8.º, 9.º, § 1.º, § 2.º, § 3.º, 11, II, § 2.º, 14, § 1.º, § 3.º, § 5.º, 15, III, 18, VI, VIII- IX, § 2.º, 19, § 3.º, 27, I, e 33, VIII, da LGPD.

3.2.3 Privacidade contextual: a integridade e o contexto na construção de normas informacionais

Considerando as diversas concepções de privacidade, Helen Nissenbaum (2004) formula o princípio da integridade contextual, tendo por base a proteção contra a vigilância pública. De acordo com esse princípio, "dependendo do contexto, diferentes aspectos da privacidade são negociados e valorizados" (BLOTTA, 2015, p. 5).

Assim, a proteção da privacidade está relacionada não ao direito subjetivo ao segredo ou sigilo, nem ao controle dos dados pessoais, mas à adequação da informação ao meio e à sua forma de distribuição ou fluxo, exigindo uma série de parâmetros, como a natureza das informações, sua relação com o contexto e suas mudanças, as regras de fluxo, tendo como ponto fundamental a análise contextual (NISSENBAUM, 2004).

Nissenbaum (2004, p. 107) ressalta que o conceito da privacidade moderna americana pauta-se por três princípios: a) limitação da vigilância dos cidadãos e do uso das informações sobre eles pelo governo; b) restrição do acesso a informações confidenciais, pessoais e privadas; c) restrição de acesso a locais considerados privados ou pessoais.

De acordo com o primeiro princípio, a preocupação com a proteção da privacidade resulta de políticas de monitoramento e de acesso a dados, especialmente na primeira geração de tratamento de dados pessoais pelo governo, a partir das décadas de 60 e 70 (3.2.1). No segundo princípio, frisa-se a proteção individual e subjetiva da privacidade da "vida privada, hábitos, atos e relações individuais" (WARREN; BRANDEIS, 1890, p. 216, tradução nossa). Por fim, o último princípio relaciona-se ao sentido patrimonial da privacidade – o lugar a ser protegido, o domínio privado. Segundo Nissenbaum (2004, p. 112), embora possam ser aplicados de forma simultânea, os princípios são independentes e suas interpretações podem mudar ao longo do tempo. Mas, tais princípios são insuficientes para abarcar a proteção da privacidade como fluxo informacional.

Helen Nissenbaum (2004, p. 120), ao definir a noção de integridade contextual, ressalta como o trânsito de informações pessoais tem um valor social, guiado por circunstâncias políticas e morais, o que determina a (im)propriedade do tráfego de dados:

> [...] contextos são parcialmente constituídos por normas que determinam e governam aspectos-chave como funções, expectativas, comportamentos e limites. Há inúmeras fontes de normas contextuais, incluindo história, cultura, direito, convenção, etc. Entre as normas presentes na maioria dos contextos estão aquelas que governam as

> informações e, o que é mais relevante para nossa discussão, as informações sobre as pessoas envolvidas nos contextos (NISSENBAUM, 2004, p. 120, tradução nossa)[108].

As normas informativas buscam identificar e proteger valores sociais que podem ser afetados pelo seu fluxo irregular. Segundo o pensamento de vários estudiosos da privacidade, a lista desses valores inclui: a) prevenção de danos informativos[109], b) desigualdade de informação[110], c) autonomia, d) liberdade[111], e) preservação de relacionamentos humanos[112] e e) democracia[113] (NISSENBAUM, 2004, p. 128).

Nesse sentido, observa-se que a análise do contexto tem por base o reconhecimento das limitações do controle do fluxo informacional, da interferência na autodeterminação informativa e da ampliação das desigualdades relacionais. Pode-se, nesses termos, afirmar que a concepção de integridade contextual reconhece a vulnerabilidade do titular no mercado informacional, retirando a força autorizadora e vinculante do consentimento do consumidor no tratamento de dados pessoais. Assim, a proteção da privacidade foca o contexto e a integridade do caso para formar a arquitetura normativa da "proteção dos dados pessoais que não se baseia única e exclusivamente nos designíos do titular" (BIONI, 2020a, p. 198).

O modelo apresentado por Nissenbaum (2004) baseia-se na identificação da violação da privacidade considerando os variados contextos e situações em que pode ser inserida. Dessa forma, a autora prescreve uma estrutura justificante quanto às restrições específicas sobre coleta, tratamento e disseminação de dados pessoais.

Ao analisar a proposta normativa em estudo, Bioni (2020a, p. 199) divide a abordagem em fluxo interno[114] (coleta e processamento de dados no acesso ao produto ou serviço) e fluxo externo[115] (compartilhamento com terceiros) na dinâmica do tráfego informacional:

---

[108] No original: "[…] contexts are partly constituted by norms, which determine and govern key aspects such as roles, expectations, behaviors, and limits. There are numerous possible sources of contextual norms, including history, culture, law, convention, etc. Among the norms present in most contexts are ones that govern information, and, most relevant to our discussion, information about the people involved in the contexts".

[109] Acesso e utilização de dados pessoais sensíveis, causando prejuízo ao titular.

[110] Desigualdade no acesso a informações e controle público-privado de dados. Nissenbaum (2004, p. 130) afirma que, na maioria das vezes, os indivíduos têm pouco conhecimento e compreensão do potencial valor de troca econômica de sua informação, não sabem o que será feito dela, não compreendem as implicações de consentir na liberação da informação e não têm o poder de reestruturar o arranjo informacional em caso de tratamento irritante, oneroso ou diferente do que inicialmente acordado.

[111] Poder de restringir o acesso às informações pessoais.

[112] Poder de controlar as informações às quais o outro terá acesso. Está relacionado com as restrições adequadas e apropriadas dos fluxos de informações individuais.

[113] Para Nissenbaum (2004, p. 132), "Privacy is a necessary condition for construction of what Erving Goffman calls 'social personae', which serves not only to alleviate complex role demands on individuals, but to facilitate a smoother transactional space for the many routine interactions that contribute to social welfare".

[114] Como exemplo, pode-se citar a coleta de dados sensíveis dos pacientes para preenchimento de prontuário médico na relação médico-paciente (NISSENBAUM, 2004; BIONI, 2020a).

[115] No caso citado na nota anterior, cabe determinar em quais condições o médico poderá compartilhar a informação (dado sensível) do paciente.

> Cada contexto tem, portanto, uma linguagem (informacional) que determina a lógica do fluxo informacional interna e externamente: internamente, quais os tipos de informações a serem trocadas entre emissário e recipiente; externamente, quem são os terceiros que podem ingressar no fluxo informacional (BIONI, 2020a, p. 201).

Zanatta (2019, p. 385), ao analisar o modelo apresentado por Nissebaum, afirma que o modelo contratualista na teoria da privacidade fracassa diante da necessidade de vincular tal direito ao fluxo apropriado de informações pessoais (não mais de controle ou sigilo). Para o autor, a integridade contextual poderá ajudar a determinar, a detectar e a reconhecer a violação, no aspecto individual e coletivista. A análise do contexto é, dessa forma, o reconhecimento da relativização da liberdade do consumidor.

A proteção de dados pessoais deverá, então, adotar parâmetros de legitimidade mais amplos do que a existência do consentimento individual prévio, considerando o contexto e as características do tratamento (MENDES; FONSECA, 2020, p. 519). A teoria, portanto, reconhece a desigualdade na relação, considera a limitação no exercício da liberdade e da autodeterminação. A privacidade contextual tem como fundamento a governabilidade da privacidade por meio de fatores contextuais na construção dos fluxos informacionais. Segundo Bioni (2020a, p. 201), a privacidade contextual consiste "na consideração de que em cada contexto o titular dos dados pessoais tem legítimas expectativas (de privacidade) de como eles irão fluir de forma apropriada" diante de um conjunto de circunstâncias que estabelecem a integridade.

3.3 A relativização da liberdade e o exercício da autodeterminação informativa

A liberdade[116] é um direito fundamental, garantido constitucionalmente[117]. Em seu artigo 170, a CF/88 destaca a liberdade como um princípio da atividade econômica. O Estado deve garantir o exercício da liberdade do consumidor, em caráter negativo ou positivo. Afirma Nunes (2017, p. 78-79):

> Primeiramente, como dissemos, o sentido de liberdade da pessoa consumidora, aqui, é o de "ação livre". Essa ação é livre sempre que a pessoa consegue acionar duas virtudes: querer + poder. Quando a pessoa quer e pode, diz-se, ela é livre; sua ação é livre. [...] Contudo, haverá casos em que, justamente por não poder escolher, a ação da pessoa não será livre. E nessa hipótese a solução tem de ser outra. Estamo-nos referindo à necessidade. O conceito é clássico: liberdade é o oposto de necessidade. Nesta não se pode ser livre: ninguém tem ação livre para não comer, não beber, para voar etc.

[116] "O conteúdo do pensamento humano, seu fundo real, não é uma criação espontânea do espírito, mas que emana sempre da experiência reflexiva das coisas reais. Portanto, o sentido racional da palavra "liberdade" é a dominação das coisas exteriores, fundada na observância respeitosa das leis da natureza e na independência frente às pretensões e atos despóticos dos homens; é a ciência, o trabalho, a revolta política, e, por fim, a organização, o modo reflexivo e livre do meio social conforme as leis naturais" (VERBICARO, 2007, p. 69).

[117] Ver os artigos 1.º (inciso IV), 3.º (inciso I), 5.º (*caput* e incisos IV, VI, IX, LIV e LXVIII) da CF/1988.

> Aplicado o conceito à realidade social, o que se tem é o fato de que o objetivo constitucional da construção de uma sociedade livre significa que, sendo a situação real de necessidade, o Estado pode e deve intervir para garantir a dignidade humana.

A liberdade envolve o exercício de opções. É o princípio garantidor do desenvolvimento da pessoa e da sua inserção na coletividade. Sem liberdade, o indivíduo não pode tomar decisões nem participar de decisões políticas fundamentais, o que provocará a exclusão social (FERREIRA, 2019, p. 57- 58).

No entanto, nas relações de consumo, é impróprio defender a "liberdade de escolha" porque ela é relativa[118] (NUNES, 2017, p. 48). Na realidade, o consumidor está exposto à condição de vulnerabilidade pela falta de igualdade material entre as partes.

Segundo Miragem (2016, p. 49), a massificação dos contratos de consumo impulsionou a uniformização das condições gerais dos contratos e dos contratos de adesão, facilitando o planejamento e a obtenção de vantagens por parte do fornecedor, mas restringindo o exercício da vontade por parte do consumidor[119].

Nesse sentido, a vontade, como força criadora de situações jurídicas nas relações privadas (PIMENTA, 1958, p. 131-135), torna-se uma liberdade relativa (ou fictícia), o risco da atividade sendo imposto ao consumidor por meio dos contratos de adesão:

> A *liberdade de contratar* e o princípio da *autonomia da vontade*, que fundamentavam o direito civil clássico, tornam-se insuficientes para assegurar a justiça e o equilíbrio nestas relações contratuais, determinando a necessidade da proteção dos mais fracos na sociedade de consumo de massas (MIRAGEM, 2016, p. 49, grifo do autor).

Assim, em razão da relativização da liberdade nas relações consumeristas, da concreta existência de desigualdades entre as partes, cabe ao Estado intervir a fim de diminuir as tensões e equilibrar a relação entre elas. De acordo com Miragem (2016, p. 50), tal "distinção implicará, necessariamente, diferenciação das normas do direito do consumidor com relação ao direito civil". A legislação consumerista mitiga os efeitos da vontade e estabelece limites para o exercício da liberdade. É o dirigismo contratual[120]:

> No Direito Consumerista, a liberdade é relativizada pela própria lei, tanto é verdade que o Estado exerce verdadeiro dirigismo contratual na relação de consumo, ao se estabelecer no CDC, por exemplo, as cláusulas que serão consideradas abusivas, assim como os respectivos parâmetros de interpretação do contrato (VERBICARO, 2017, p. 213).

---

[118] Verbicaro (2017, p. 213) destaca que o aceite de uma condição contratual, desigual ou abusiva, está relacionado à satisfação da necessidade de consumo e não à liberdade em si.

[119] Para Miragem (p. 49, grifo do autor), "Estas circunstâncias dão origem então ao fenômeno dos *contratos de massa*, ou simplesmente o fenômeno da *massificação dos contratos*, pelo qual a adoção de práticas agressivas de contratação e a sensível restrição da liberdade de contratar de uma das partes (os não profissionais, leigos) assinalam a debilidade destes sujeitos na relação contratual, indicando a necessidade do reconhecimento desta situação pelo direito, de modo a promover a proteção do vulnerável".

[120] *Vide* o artigo 51 do CDC sobre nulidades de cláusula contratual.

O dirigismo contratual ou contrato dirigido acentua a interferência direta do legislador de modo a substituir por cláusulas legais e regulamentares o livre ajuste entre as partes (PIMENTA, 1958, p. 135). No direito do consumidor, a condição de vulnerabilidade impõe o tratamento protetivo.

Diante da relativização da liberdade e da consequente ausência do absoluto controle sobre os dados pessoais na economia de dados, discute-se a efetivação do consentimento ativo na economia de dados em razão da engenheira algorítmica que envolve todo o ciclo mercadológico das informações pessoais. No entanto, em razão do desequilíbrio relacional e do reconhecimento da vulnerabilidade nas relações consumeristas, o exercício da plena liberdade e a consequente autodeterminação informacional na concessão do consentimento são prejudicados.

O consentimento e a autodeterminação informativa tornaram-se os grandes protagonistas no processo de coleta, tratamento e distribuição de dados pessoais. No entanto, é fato que a participação ativa e individual do consumidor deve abranger, além das estratégias regulatórias, a reavaliação procedimental.

No capítulo seguinte, serão abordadas as formas legítimas que autorizam o tratamento de dados pessoais, bem como a responsabilidade pelo uso indevido de dados. Diante de tantas lacunas protetivas na relação consumerista, uma das armas contra a vulnerabilidade do consumidor é seu consentimento.

4 O PAPEL DO CONSENTIMENTO NA PROTEÇÃO DE DADOS DE CONSUMO

4.1 Bases legais autorizadoras do tratamento de dados pessoais

Na análise da LGPD – Lei n.º 13.709/2018 –, é possível identificar cinco eixos principais: a) unidade e generalidade da aplicação da lei; b) hipóteses autorizativas; c) princípios e direitos do titular de dados pessoais; d) obrigações dos agentes de tratamento; e) reponsabilidade (MENDES; DONEDA, 2018, p. 471-472). No que diz respeito à sua aplicação, a LGPD aplica-se à pessoa natural, no âmbito público e privado, abrangendo o tratamento dos dados no ciberespaço.

Da análise dos artigos 7.º e 23 da LGPD, infere-se que há 11 hipóteses autorizativas[121] do tratamento de dados pessoais.

O tratamento de dados pessoais para cumprir obrigação legal ou regulatória está estabelecido no artigo 7.º, II, da LGPD. É admitido, pois, o tratamento de dados pessoais sem o consentimento do titular em obediência a lei específica ou regulamento, sendo dispensada, nesse caso, a obrigação de informar.

Quanto ao tratamento de dados para execução de políticas públicas, em atenção ao artigo 7.º, III, da LGPD, somente pode ser realizado pela administração pública, o que exclui o tratamento de dados pessoais por empresas privadas, mesmo que estejam inseridas nessas políticas públicas (COTS; OLIVEIRA, 2020, p. 53). Essa possibilidade é criticada por Wimmer (2019, p. 131):

> Saltam aos olhos, de imediato, dois problemas: um relacionado ao âmbito subjetivo da hipótese autorizativa e outro relacionado ao seu âmbito material. Conforme amplamente debatido anteriormente, o Poder Público não se resume à Administração Pública e as inúmeras atividades por ele desempenhadas transcendem, em grande medida, a execução de políticas públicas.
> De fato, por meio de suas diferentes ramificações no âmbito do Executivo, do Legislativo e do Judiciário, o Poder Público ocupa-se de uma miríade de atividades envolvendo o exercício de poder de polícia administrativo, a realização de pagamentos, a gestão de servidores públicos e a prestação de tutela jurisdicional, para citar apenas alguns exemplos que dificilmente podem ser caracterizados como execução de políticas públicas. Embora o princípio da legalidade, que norteia todas as atividades públicas, imponha que tais atividades possuam amparo legal, resta a questão de saber qual ou quais seriam as bases legais específicas da LGPD para fundamentar o tratamento de dados pessoais associado a tais funções.

A possibilidade de realização do tratamento de dados pelo poder público no exercício geral de suas competências ou para cumprimento de atribuição legal está descrita no artigo 23 da LGPD, observadas as limitações atinentes:

---

[121] Para o tratamento de dados sensíveis, são oito as suas bases legais.

> Art. 23. [...]
> I - 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;
> [...]
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; [...].

Assim, é autorizada a realização de tratamento de dados pessoais pelo Estado em duas hipóteses: a) políticas públicas; b) exercício de suas competências e atribuição legal em atenção à dimensão social que pode ser influenciada por tais hipóteses legislativas.

Ainda, o artigo 7.º, IV, da LGPD admite o tratamento de dados para realização de pesquisa, desde que garantida a anonimização dos dados pessoais. O inciso V prevê a realização de tratamento de dados pessoais quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a negócio jurídico do qual seja parte o titular dos dados. O inciso V autoriza, portanto, o trato de dados pessoais na fase pré-contratual, em procedimentos preliminares, desde que a pedido do titular.

De acordo com o artigo 7.º, VI, da LGPD, poderá ser realizado "o tratamento de dados pessoais sempre que tiver um direito previsto em lei, regulamento ou em decorrência da arbitragem" (COTS; OLIVEIRA, 2020, p. 54). O artigo 7.º garante o tratamento de dados para a proteção da vida e da incolumidade pública (inciso VII) e para a proteção da saúde (inciso VIII). Nesse último caso, há expressa menção aos procedimentos realizados por profissionais de saúde, serviços de saúde, pública ou privada, ou autoridade sanitária.

Para a proteção do crédito, prevista no artigo 7.º, X, da LGPD, o tratamento de dados pessoais pode ser realizado "de forma automática, sem o consentimento e amplo controle dos indivíduos frente à Lei do Cadastro Positivo" (FREITAS; MAFFINI, 2020, p. 41). Conforme o artigo 4.º da Lei do Cadastro Positivo (LCP), o gestor de banco de dados está autorizado a abrir cadastro, fazer anotações, compartilhar informações cadastrais e de adimplemento armazenadas e disponibilizar nota ou pontuação de crédito e/ou histórico de crédito, mediante prévia autorização específica do cadastrado, desde que garanta a transparência e o controle, especialmente quanto aos direitos de revisão, em atenção ao artigo 20 da LGPD.

O legítimo interesse está disposto nos artigos 7.º, IX, 10.º e 37 da LGPD. Não há definição expressa para essa base legal, porém, é possível verificar os requisitos para sua aplicação nos termos do artigo 10.º da LGPD: interesse do controlador, finalidade legítima, situações concretas, proteção dos direitos do titular, legítima expectativa e princípios da

necessidade e transparência (COTS; OLIVEIRA, 2020, p. 66). Ainda, em atenção ao artigo 47 da LGPD, o legítimo interesse pode ser estabelecido em razão de uma relação jurídica prévia.

Para Joelsons (2020, p. 13), o caráter proposital do hiato conceitual da base legal possibilita uma aplicação concreta, flexível e ampla. A expressão "finalidades legítimas" (artigo 10.º da LGPD) relaciona-se ao objeto ou ao propósito do tratamento; nesses casos, o tratamento de dados é fundamentado na lei ou em outra fonte do direito, a partir da análise de situações e contextos concretos. No mesmo sentido, segue a interpretação da expressão "legítima expectativa". No que diz respeito ao interesse do controlador, a legislação, de forma exemplificativa, pontua, nos incisos I e II do artigo 10.º, a observância do princípio da boa-fé.

Para Joelsons (2020, p. 4), "um interesse pode ser considerado legítimo desde que o responsável pelo tratamento possa prosseguir esse interesse em conformidade com a legislação em matéria de proteção de dados e demais legislações aplicáveis". A autora ainda destaca a necessidade de confiança na atividade do controlador para a concretude do legítimo interesse (JOELSONS, 2020, p. 2).

Nas relações consumeristas, o legítimo interesse é uma alternativa contra o consentimento relativizado. No entanto, é necessário estabelecer o "equilíbrio provisório" entre as partes por meio de mecanismos que garantam a exclusão de seus dados ou *opt out* (COTS; OLIVEIRA, 2020, p. 153), a transparência em todo o processo de tratamento de dados, bem como o teste de proporcionalidade entre os interesses recíprocos à luz da boa-fé. Nesse sentido, tecnologias que privilegiam o PbD (subseção 5.3) devem ser adotadas na busca da autodeterminação informativa.

O princípio da necessidade e o da transparência estão taxativamente dispostos nos § 1.° e § 2.º do artigo 10.º da LGPD. O primeiro diz respeito à pertinência do dado para buscar a finalidade específica; no segundo caso, permite-se que o titular dos dados pessoais controle suas informações a fim de garantir o direito à oposição, uma vez que tal base legal está desatrelada do consentimento do titular.

Em seus artigos 5.º, XII e 11, I, a LGPD estabeleceu parâmetros para a concretude, a função e os limites do consentimento. O presente estudo tem por objeto analisar a admissão dessa base no tratamento de dados de consumo, como se verá a seguir.

4.2 O consentimento e sua função na economia de dados pessoais

Nos termos do artigo 7°, I, da LGPD, o consentimento é uma das bases normativas para a concessão de dados pessoais. Desde o seu reconhecimento, na terceira geração, o

consentimento representa o paradigma "utilizado para legitimar, justificar e alicerçar a proteção de dados pessoais" (MENDES; FONSECA, 2020, p. 513). O consentimento tornou-se o precursor da suposta materialização da autonomia do consumidor no contexto de coleta e tratamento de dados.

Em 1970, surgiram séries de princípios sob a denominação *fair information practices* que se tornaram diretrizes da Organização para Cooperação e Desenvolvimento Econômico (OCDE) sobre a proteção transfronteiriça de dados pessoais em 1980 (CATE; MAYER-SCHÖNBERGER, 2013, p. 67). Considerando tais diretrizes, um dos principais fundamentos legais para a concessão e o tratamento de dados pessoais seria o consentimento informado[122].

Contudo, na quarta geração das leis protetoras de dados pessoais, passou-se a admitir a relativização do consentimento. Isso se dá pelo reconhecimento das desigualdades entre as partes, concretizadas na caracterização das vulnerabilidades do consumidor, como, por exemplo, na imposição da tomada de decisão bifásica sobre questões complexas face das informações qualificadas limitadas.

Cate e Mayer-Schönberger (2013, p. 70-71) enumeram desafios significativos relacionados à proteção de dados pessoais com base nas diretrizes estruturantes da OCDE: a) maior conscientização pública sobre questões que envolvem a proteção da privacidade, maior transparência no uso de dados pessoais e uma educação mais eficaz sobre privacidade; b) maior padronização, consistência e interoperabilidade entre leis e práticas de proteção de dados em âmbito global; c) equilíbrio entre a proteção de dados e o livre fluxo de informações; d) necessidade de termos claros e de definições específicas para os usuários; e) aprimoramento das leis de proteção de dados com base nas diretrizes da OCDE.

Segundo Bioni (2020a, p. 112), apesar do progresso no reconhecimento das limitações do consentimento e das discussões sobre a necessidade de atualização, o consentimento não perdeu sua centralidade e seu protagonismo. O Regulamento 2016/679 da União Europeia (2016) admite o tratamento de dados pessoais desde que embasado no consentimento legítimo, informado, livre e mutável[123]. No mesmo sentido, a LGPD, no seu artigo 5º, XII, vinculou o

[122] "Princípio de limitação de utilização: 10. Dados pessoais não deveriam ser divulgados, comunicados ou utilizados com finalidades outras das que foram especificadas de acordo com o Parágrafo 9, salvo: 1. com o consentimento do sujeito dos dados; ou 2. por força de lei" (ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICOS, 2002, p. 4).

[123] "Artigo 7.º Condições aplicáveis ao consentimento 1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais. 2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento. 3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer

consentimento livre, informado, inequívoco, explícito e/ou específico a uma finalidade determinada.

O consentimento, ao sistematizar a atuação da autonomia privada, deverá tomar forma da manifestação da escolha do consumidor e, ao mesmo tempo, fazer referência direta aos valores em questão. Em um sistema patrimonialista, o consentimento ganha o caráter legitimador do tratamento de dados. Na visão personalíssima, está relacionado ao exercício da liberdade negativa e da autodeterminação informativa, é instrumento do exercício de poder (DONEDA, 2019, p. 297-298; MENDES, 2019, p. 63).

Na economia de dados, o consentimento transmuta "a informação pessoal em um bem jurídico – na possibilidade de concedê-lo ou negá-lo, e reside exatamente nesse poder, caso limitado de alguma forma em uma estrutura negocial, perderia sua razão de ser" (DONEDA, 2019, p. 302). É expressão da autodeterminação por manifestar a vontade de autorizar o processamento de dados pessoais (MENDES, 2019, p. 60) e é instrumento de legitimação do tratamento de dados.

No entanto, o fluxo informacional do consumidor (subseção 2.4) é de difícil racionalização na economia de dados, concretiza vulnerabilidades (subseção 3.1) diante da complexa engenharia de mineração de dados:

> A própria lógica do *trade-off* da economia dos dados pessoais é traiçoeira, portanto, frente a tal arquitetura de escolha de decisões, notadamente por essa idiossincrasia entre gratificações imediatas e prejuízos mediatos/distantes. A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno e tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo de informações pessoais (BIONI, 2020a, p. 141).

No mesmo sentido, Mendes e Fonseca (2020, p. 513-514) apontam três insuficiências limitadoras do exercício do consentimento:

> (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular como, por exemplo, em circunstâncias denominadas "take it or leave it"; e (iii) as modernas técnicas de tratamento e análise de dados a partir de *Big Data* que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido.

As limitações cognitivas estão relacionadas à vulnerabilidade psicocomportamental (3.1.2) do consumidor inserido no contexto de tratamento de dados pessoais. Os *insights* e

momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar. 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato" (UNIÃO EUROPEIA, 2016).

heuristicas utilizados na abordagem assediadora exploram o impulso e a persuasão que, atrelados à vulnerabilidade algorítmica (3.1.4), influenciam o ato de consentir viciado e relativizado.

A segunda insuficiência destacada pelos autores concerne à desigualdade entre os atores da relação, o que estabelece uma concreta assimetria, especialmente de poder. Como visto na análise da vulnerabilidade situacional (3.1.3), o consumidor encontra-se em uma circunstância em que não concordar com os termos de privacidade impede a utilização do produto e/ou serviço.

Por fim, a terceira insuficiência diz respeito ao complexo fluxo e rede de atores que participam do tratamento de dados, que dificulta a compreensão do consumidor médio acerca da engenharia tecnológica usada.

Para Solove (2013, p. 1880-1881), a autogestão da privacidade não garante o controle necessário dos dados pessoais. Isso porque existem problemas que inviabilizam tal gestão, como questões cognitivas do usuário, questões estruturais, dificuldade de compreender a alta complexidade das redes de informação, falta de consciência de que o consentimento individual para dados pessoais produzirá efeitos coletivos, sociais.

Solove (2013, p. 1883) afirma que os problemas cognitivos são fruto da desinformação e da distorção na tomada de decisão – essa última relacionada com a decisão baseada em heurísticas e a estruturação das escolhas:

> Os problemas cognitivos acima apresentam, portanto, vários obstáculos para a autogestão da privacidade: (1) as pessoas não leem as políticas de privacidade; (2) se leem, não as entendem; (3) se leem e entendem, muitas vezes não têm conhecimento prévio suficiente para fazer uma escolha informada; e (4) se leem, entendem, podem fazer escolhas informadas, sua escolha pode ser distorcida por várias dificuldades na tomada de decisão (SOLOVE, 2013, p. 1888, tradução nossa)[124].

Como problemas estruturais do consentimento, Solove (2013, p. 1888-1893) destaca a escala – relacionada ao conhecimento sobre a quantidade de atores que tratam uma coleta de dados –, a agregação – impossibilidade de identificação da possível combinação de dados para a revelação de dados sensíveis – e a avaliação de danos – dificuldade em analisar o custo-benefício futuro para autorizar a coleta de dados.

Assim, a assimetria informacional e de poder na relação de dados de consumo gera marcadores vulnerabilizantes no usuário-consumidor inserido nesse contexto. O consumidor

[124] No original: "The cognitive problems above thus present numerous hurdles for privacy self-management: (1) people do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties".

não tem conhecimento da real implicação do consentimento e, por vezes, dispõe das suas informações por conveniência, incentivos e/ou descontos. Tal ação inócua e ilusória caracteriza o "mito do consentimento" (DONEDA, 2019; MALHEIRO, 2017, p. 56), bem como o dito paradoxo da privacidade pela busca da tutela dos dados pessoais a partir da autorização do próprio consumidor[125].

De outro modo, a desigualdade da relação consumerista reconhece a liberdade mitigada (3.3) e a consequente relativização da autonomia da vontade. Diante das condições vulnerabilizantes já apresentadas, cabe questionar o protagonismo do consentimento do consumidor nas legislações.

Para Podestà (2019, p. 98-99), a natureza da concessão de dados pessoais não pode ser atrelada à natureza negocial, deve antes estar ligada à máxima racionalidade para atender os interesses dos usuários consumidores. Para isso, com o objetivo de reforçar a primazia da transparência-informação-controle estabelecida na LGPD, medidas alternativas, adicionais e suplementares à lei, devem ser impostas para retirar o protagonismo do consentimento.

Isso porque, no mercado informacional, a assimetria relacional fragiliza o exercício do consentimento ativo, configurando vício de consentimento e possibilitando a anulabilidade do negócio jurídico[126]. Ademais, as políticas de privacidade escancaradas por contratos de adesão impossibilitam o exercício da vontade, sendo as nulidades de cláusulas contratuais abusivas, nos termos do artigo 51 do CDC, medidas paliativas na proteção de dados pessoais. É o caso de "investigar como a tecnologia poderia massificar as escolhas dos consumidores sobre o trânsito de seus dados pessoais para toda a miríade de atores do mercado informacional" (BIONI, 2020a, p. 166).

O consentimento ativo só é realizado quando o consumidor tem total conhecimento da implicação da disponibilização de seus dados para possibilitar o exercício da vontade[127] (ROCHA; MAZIVIERO, 2020). É o aceite livre, informado, inequívoco e explícito, esse último quando se tratar de dado sensível, reflexo do direito da autodeterminação informacional, que consiste em conhecer o uso de suas informações por terceiros, controlá-los e impedi-los (CARVALHO, 2003, p. 6).

---

[125] Mendes (2019, p. 60-65) aponta o paradoxo da privacidade ao relacionar a busca da tutela jurídica da privacidade após a autorização para o tratamento de dados.

[126] Artigo 138 do CC/2002: "São anuláveis os negócios jurídicos, quando as declarações de vontade emanarem de erro substancial que poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio".

[127] Em decisão da Corte Europeia, em 1.º de outubro de 2019, no processo C-673/17, cujas partes são *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV* contra *Planet19 GmbH*, foi estabelecido que, em todas as etapas da coleta de dados pessoais, deve ser possibilitado o direito à informação e à efetividade do consentimento ativo do consumidor.

No mesmo sentido, segundo Fortes (2016), o consentimento colaborativo (ativo) é aquele considerado interativo e dinâmico, no processo de interação na internet, o que garante os principais direitos quando se analisa a utilização do ciberespaço, como o direito de navegar pela internet com privacidade, o direito de monitorar quem monitora, o direito de deletar os dados pessoais, o direito a uma identidade *on-line*, nos termos estabelecidos pela LGPD e pelo CDC. Ressalta-se que o consentimento ao tratamento de dados sensíveis tem por base um tratamento específico e destacado para finalidades singulares[128] (MULHOLLAND, 2019, p. 50).

Lima (2019, p. 62) lembra que o consentimento ativo granular, durante as diversas fases da coleta, de acordo com as etapas de utilização do serviço, possibilita, a qualquer tempo, a sua revogação (*opt-out*). Esse consentimento deve expressar uma vontade refletida por meio de uma ação informada e expressa em uma relação transparente.

A transparência na arquitetura de rede de informações, bem como o exercício do direito-dever da informação, portanto, possibilitarão a redução do desequilíbrio relacional e o consequente empoderamento do consumidor no exercício ativo do seu consentimento. A LGDP e o CDC impõem práticas transparentes na busca da redução das assimetrias informacional e de poder no tratamento de dados de consumo. Esse empoderamento consumerista ultrapassa a aplicação das normas vigentes, mas reside no compartilhamento de autoridade política, como se verá no capítulo 5, seja no exercício ativo do Estado, como mediador da relação, seja na aplicação de uma engenharia tecnológica de proteção de dados pessoais, em que a privacidade do usuário-consumidor está no centro, desde a concepção da estruturação da atividade.

4.3 O diálogo das fontes: a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) e o Código de Defesa do Consumidor (Lei n.° 8.078/1990)

A teoria do diálogo das fontes foi elaborada por Erik Jayme e por ele apresentada no seu Curso Geral ministrado em Haia em 1995 para explicar o pluralismo das fontes e o fenômeno da comunicação. A professora Cláudia Lima Marques adaptou-a ao direito brasileiro. Tal teoria estabelece a "aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas,

[128] Para Mulholland (2019, p. 51), "por exemplo, deve-se especificar que a coleta por uma seguradora de saúde de dados sobre doenças preexistentes só estará legitimada se restrita a essas informações – doenças preexistentes – estando excluídas de tratamento todas as demais informações sobre a situação de saúde do contratante". É importante frisar que, no que diz respeito à coleta e ao tratamento de dados sensíveis, a LGPD exige a concordância expressa. Diversamente do tratamento dos demais dados pessoais, pela caracterização da ação inequívoca, caso o titular tenha condutas incompatíveis com a recusa do tratamento de dados, é possível considerar o seu consentimento (LIMA, 2019, p. 63-65).

internacionais, supranacionais e nacionais leis especiais e gerais, com campos de aplicação convergentes, mas não mais iguais, daí a impossibilidade de revogação, derrogação ou ab-rogação" (BENJAMIN; MARQUES, 2018, p. 23). Portanto, o diálogo das fontes expressa a necessidade de comunicação entre normas convergentes para resgatar valores de direitos humanos, de forma subsidiária ou complementar.

Benjamin e Marques (2018, p. 27-28) apresentam três principais sentidos do diálogo: a plasticidade contra a rigidez metodológica da aplicação das normas; a convivência de paradigmas e o aproveitamento recíproco; a harmonia na pluralidade de fontes no sentido de buscar uma coerência entre valores constitucionais e fundamentais. O diálogo representa, portanto, uma solução flexível e aberta mais favorável para a proteção dos direitos humanos e dos agentes considerados mais vulneráveis na relação.

O artigo 7.º do CDC[129] respeita esses sentidos ao estabelecer a aplicação conjunta das leis em favor do consumidor. Cumpre destacar a inclusão do § 2.º nesse artigo por meio do PL 281/2012 para que seja aplicada a norma mais favorável ao consumidor. No entanto, a redação substitutiva do referido projeto no Senado, por meio do PL 3514/2015, retirou o parágrafo vinculado ao artigo 7.º e propôs a criação do artigo 3.º-A no mesmo sentido. Segundo Benjamin e Marques (2018, p. 38), a mudança não trouxe prejuízo ao conteúdo, mas acarretou a perda da possível valoração da função sistematizadora e pedagógica do artigo 7.º citado.

No mesmo sentido, o artigo 64 da LGPD[130] estabelece a aplicação dialogada entre leis e tratados internacionais ao defender a não exclusão dos princípios e direitos expressos por outras legislações. Para Miragem (2019a, p. 2), trata-se da "adoção expressa da interpretação sistemática segundo a técnica do diálogo das fontes".

Marques (2003, p. 2-3) apresenta três tipos de diálogos possíveis entre fontes: a) aplicação simultânea de duas leis – diálogo sistemático de coerência; b) a aplicação coordenada de duas leis – diálogo sistemático de complementaridade e subsidiariedade; c) a redefinição do campo de aplicação da lei – diálogo das influências recíprocas sistemáticas.

Barasuol Junior (2020, p. 90-91) entende que o diálogo entre o CDC e a LGPD visa coordenar as normas para criar uma estrutura de proteção do vulnerável na relação, na tentativa de restaurar a coerência, amenizar a complexidade e utilizar conceitos consolidados em matéria

[129] "Art. 7.º Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e equidade".

[130] "Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte".

consumerista. Para isso, o autor recorre a três formas de interpretação sistemática das normas: a) coerência – observância dos princípios constitucionais; b) complementaridade ou subsidiariedade; c) adaptação e coordenação – influência recíproca de conceitos estruturais.

Este trabalho visa destacar pontos de convergência na interpretação sistemática da LGPD e do CDC que garantam proteção ao consumidor ante sua vulnerabilidade, reconhecida em ambas as leis.

4.3.1 A caracterização do consentimento ativo à luz da base principiológica da legislação

A LGPD, em seu artigo 5.º, XII, define consentimento como uma ação livre, informada, inequívoca e com finalidade determinada. O tratamento de dados sensíveis exige um consentimento específico e expresso. No mesmo sentido, Mendes (2019, p. 65) assevera:

> Pode-se dizer que os pressupostos de um consentimento válido, no âmbito de proteção de dados, são os seguintes: i) que o titular dos dados que emita o consentimento o faça por livre vontade; ii) que o consentimento seja voltado a uma finalidade específica; iii) que o titular seja informado acerca do objetivo da coleta, processamento e do uso dos dados, assim como das consequências de não consentir.

O direito-dever de informar significa "compreender os riscos e as implicações que tal atividade trará sobre a sua esfera pessoal, a fim de racionalizar alguma decisão sobre o fluxo de seus dados" (BIONI, 2020a, p. 181). A LGPD segue essa premissa ao a) prescrever a informação como clara, adequada e ostensiva (aspecto qualitativo) e b) elencar os tipos de informação que devem estar presentes do processo comunicativo (aspecto quantitativo) (BIONI, 2020a, p. 182).

O dever-direito à informação deve embasar a tomada de decisão legítima, ligada ao exercício da transparência. O objetivo é tornar a relação menos obscura e assimétrica (BIONI, 2020a, p. 184-185).

No âmbito do projeto CONSENT, vinculado à Universidade de Malta, Custers *et al.* (2013, p. 438) apresentam uma tabela com os critérios adotados para determinar se houve consentimento informado.

Tabela 1 – Critérios de consentimento.

Critérios para a decisão de consentir	Critérios relativos à pessoa que consente	C1.1	A pessoa que consente é adulta? Se não, há o consentimento dos pais?
		C1.2	A pessoa que consente é capaz de consentir? Se não, há o consentimento de seu representante legal?
		C1.3	A pessoa que consente é competente para consentir?
	Critérios para o modo como é dado o consentimento	C2.1	É escrito?
		C2.2	O consentimento é parcial ou total? Se parcial, o consentimento atende ao propósito comunicado?
		C2.3	O consentimento é razoavelmente forte?
		C2.4	O consentimento é fruto de uma decisão independente?
		C2.5	O consentimento é atualizado?
Critérios para o discernimento na decisão do consentimento	Critérios relativos às informações que devem ser disponibilizadas ao usuário	C3.1	Está claro quais dados são coletados, usados e compartilhados?
		C3.2	Os objetivos são claros?
		C3.3	Estão claras as medidas de segurança tomadas?
		C3.4	Está claro quem processa os dados e quem é responsável por eles?
		C3.5	Estão claros os direitos que podem ser exercidos? Está claro como esses direitos podem ser exercidos?
	Critérios para o modo de fornecer as informações ao usuário	C4.1	A informação é específica e suficientemente detalhada?
		C4.2	A informação é compreensível?
		C4.3	A informação é precisa e confiável?
		C4.4	A informação é acessível?

Fonte: CUSTERS *et al.*, 2013, p. 438, tradução nossa.

O exercício livre é a racionalização da intenção na tomada de decisão, ou seja, "a concepção de ato volitivo [...] deve não ser fruto de coação (física ou moral), a fim de que a autodeterminação informativa seja vetorizada de forma genuína" (BIONI, 2015, p. 44).

A finalidade determinada implica que o tratamento dos dados necessariamente atenda a um propósito definido. É importante notar que a expressão "finalidade" está relacionada às possibilidades do contexto e não a uma situação específica em si. Bioni (2015, p. 45) exemplifica: "em serviços de internet banking seria razoável que os dados pessoais dos

consumidores fossem tratados não só para operacionalizar o próprio serviço em si de transferências financeiras, como, também, para prevenção de fraudes".

O consentimento inequívoco não faz menção ao ato expresso. É possível um consentimento tácito desde que extraído do contexto relacional, salvo, como já afirmado, no caso de tratamento de dados sensíveis. Leonardi (2019, p. 321) aduz:

> A adoção do consentimento inequívoco como regra, em oposição a específico e destacado (ou expresso como mencionado pela Lei 12.965/2014 – Marco Civil da Internet), viabiliza o tratamento de dados no ambiente online, permite a contínua inovação baseada em dados e assegura um nível de proteção adequado ao titular sem gerar ônus excessivos para os responsáveis pelo tratamento de dados.

Na assimetria relacional, caracterizada pelo exercício de poder e pela informação discrepante, deve ser garantido ao consumidor o exercício da liberdade na realização do seu consentimento. No entanto, em caráter não apenas meramente formal, mas também material (MENDES, 2019, p. 65).

São pressupostos para conferir o exercício do controle das informações pessoais. O consentimento ativo está ligado aos direitos básicos dos titulares de dados: acesso, retificação, cancelamento, explicação e transparência.

Definido no artigo 18, II, da LGPD, o direito de acesso permite que o titular dos dados pessoais possa ter acesso às suas informações. A LGPD distingue o acesso a informações simplificadas e a informações completas. No primeiro caso, o controlador deverá informar a existência e os tipos de dados tratados. Já no segundo, além das informações contidas no primeiro tipo, o controlador deverá fornecer a origem, os critérios e a finalidade do tratamento dos dados, tendo, como limitações, o segredo comercial e industrial. Ainda, as informações devem ser fornecidas num formato que facilite seu uso posterior (em caso de portabilidade ou de usos próprios).

O artigo 43 do CDC garante ao consumidor o direito de acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados e a capacidade de autodeterminar suas informações pessoais (BIONI, 2020a, p. 121):

> a) Garantir o seu acesso pelo consumidor (art. 43, *caput*, do CDC); ii) exatidão de tais informações; iii) que o banco de dados se restrinja *para finalidades claras e verdadeiras* e, por fim; iv) que seja observado o limite temporal de cinco anos para armazenamento de informações negativas (art. 43, 1.º, do CDC) (BIONI, 2020a, p. 122).

O direito de retificação, nos termos do artigo 18, inciso III, da LPDC, garante ao titular a possibilidade de solicitar a correção de dados incompletos, inexatos ou desatualizados de natureza objetiva – erro formal – ou subjetiva – atualização de relatórios e informações, salvo os dados anonimizados. Em caso de retificação, o responsável deverá solicitar imediatamente

aos agentes de tratamento com os quais tenha compartilhado dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, cabendo ao controlador (o que recebeu a informação) comunicar todos os agentes de tratamento para que realizem a retificação.

O direito de cancelamento envolve a eliminação dos dados pessoais tratados com o consentimento do titular. A conservação é autorizada para cumprimento de obrigação legal ou regulatória pelo controlador, para estudo por órgão de pesquisa – garantida, sempre que possível, a anonimização dos dados pessoais –, para transferência a terceiro ou para uso exclusivo do controlador, vedado seu acesso por terceiro, desde que anonimizados os dados.

O direito de cancelamento não é absoluto por causa das limitações técnicas estabelecidas nos artigos 16 e 18, § 6.º, da LGPD. Caso o consumidor solicite o cancelamento e isso não for possível, os dados podem ser anonimizados. Os fornecedores podem manter os dados para os argumentos de defesa em processo, sem, no entanto, poder utilizá-los para outras finalidades.

O direito à explicação relaciona-se à incidência da transparência e ao direito à informação. Devem ser fornecidas informações claras, precisas e diretas sobre o tratamento dos dados. Não há prazo para isso, mas a demora deve ser justificada.

Para Mendes (2019, p. 71), a transparência é uma das principais condições do combate aos abusos. É nítida a necessidade da caracterização da transparência na relação, pois ela está diretamente ligada à garantia do direito ao pleno conhecimento do fluxo dos dados pessoais, possibilitando, assim, o exercício da autodeterminação informativa, em observância ao disposto na LGPD e no CDC.

A transparência não deve ser justificativa para vincular o consentimento a um processo bifásico. É importante frisar a importância do estabelecimento de uma arquitetura de rede que possibilite o consentimento granular de acordo com a utilização menos invasiva e coercitiva do produto ou do serviço, configurando, portanto, limites com base em autorizações fragmentadas (BIONI, 2015, p. 55). Isso dá ao consumidor um poder de barganha para disponibilizar seus dados de acordo com as funcionalidades a serem adotadas.

4.3.2 Responsabilidade civil por uso indevido e irregular de dados

No que diz respeito às novas formas de responsabilização dos agentes de tratamento de dados pessoais, podem-se apontar duas situações de responsabilidade civil na LGPD: a) violação de normas jurídicas; 2) violação de normas técnicas, voltadas para a segurança e a proteção de dados pessoais (CAPANEMA, 2020). Bonna (2020, p. 20) afirma que as hipóteses

ensejadoras de responsabilidade civil têm por fundamento evitar o dano-evento – a violação de um dever na ordem jurídica – e o dano-prejuízo – consequências danosas existenciais e morais decorrentes do dano-evento.

Tratando-se de relação de consumo[131], o dever de indenizar, pela caracterização do vício ou defeito, exige a demonstração do tripé fato-nexo de causalidade-dano, sem a necessidade de demonstração de culpa. A LGPD apresenta um carater binário de responsabilização, ou, como dizem Bioni e Dias (2020, p. 21), "um regime jurídico de responsabilidade civil subjetiva com alto grau de objetividade".

Como se viu, a responsabilidade será configurada quando houver tratamento de dados irregular causado por inobservância da legislação ou "quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes", conforme o *caput* do artigo 44 da LGPD. A grande questão é: o tratamento irregular que enseja responsabilização segundo a lei pode ser entendido, ao mesmo tempo, como violação da lei e como violação da segurança?

Segundo Bioni e Dias (2020, p. 10), a considerada má técnica legislativa pode ser parcialmente explicada pela transposição para a LGPD da previsão do CDC que regula o defeito do serviço.

Tabela 2 – Comparação: CDC *versus* LGPD.

CDC	**LGPD**
Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. § 1.º O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais: **I - o modo de seu fornecimento;** **II - o resultado e os riscos que razoavelmente dele se esperam;** **III - a época em que foi fornecido.** § 2.º O serviço não é considerado defeituoso pela adoção de novas técnicas. § 3.º O fornecedor de serviços só não será responsabilizado quando provar: I - que, tendo prestado o serviço, o defeito inexiste; II - a culpa exclusiva do consumidor ou de terceiro. § 4.º A responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa.	Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: **I - o modo pelo qual é realizado;** **II - o resultado e os riscos que razoavelmente dele se esperam;** **III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado**. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

Fonte: BIONI; DIAS, 2020, p. 11, grifo nosso.

[131] Destaca-se que a LGPD prioriza o tratamento de dados de pessoa natural, excluindo, dessa maneira, os dados de pessoa jurídica. Nas relações de consumo, há a possibilidade de considerar a pessoa jurídica consumidora em atenção à teoria maximalista e finalista mitigada.

Constata-se a concreta utilização do CDC na caracterização do produto defeituoso, com nítida referência à configuração do que se pode esperar de insegurança. No mesmo sentido, Miragem (2021, p. 488) aproxima a LGPD do CDC na configuração do fato do produto ou serviço, “em especial na definição dos critérios a serem considerados para determinação do atendimento ao dever de segurança” em observância à previsibilidade de atualização e de avanço técnico atinente à atividade.

Em outro sentido, o parágrafo único do artigo 44 da LPGD estabelece a responsabilização do agente que “deixar de adotar as medidas de segurança previstas no artigo 46 desta Lei”, o que vincula a caracterização de medida de segurança à adoção dos pressupostos indicados no citado artigo. Bioni e Dias (2020, p. 12, grifo dos autores) ressaltam:

> Por outro lado, é bem mais frutífera a análise do critério de irregularidade do tratamento “quando não fornecer a segurança que o titular dele pode esperar”. Mas o que isso significa exatamente? Em primeiro lugar, não é a segurança cujo fornecimento de fato se espera, mas sim aquela que se “pode esperar”. No primeiro caso, seria uma mera constatação fática. No segundo, há aí um *filtro jurídico*: aquilo que, do ponto de vista jurídico, o titular está autorizado a esperar. Não se trata de qualquer expectativa de segurança, mas sim de expectativas juridicamente legítimas. Vai-se trabalhar aqui, assim como se trabalha no CDC, com “legítimas expectativas de segurança”.

Para a doutrina consumerista, a legítima expectativa está relacionada à expectativa de segurança do produto ou serviço, diretamente em confronto com o estado da técnica e as condições econômicas na época. Caso contrário, corresponderá a uma periculosidade adquirida, ou seja, a um defeito (BENJAMIN, 2009, p. 117).

Para definir a responsabilidade por produto defeituoso ou vício de qualidade por insegurança (fato do serviço), o CDC adota o critério objetivo – o dano concreto, de caráter físico ou psicológico, ao consumidor. No que diz respeito à proteção de dados, a doutrina age de forma análoga, em consonância com o caso concreto (BIONI; DIAS, 2020, p. 15).

No que diz respeito às circunstâncias relevantes apresentadas nos incisos I, II e III do artigo 44 da LGPD, é possível interpretá-las junto com o que preceitua o artigo 50, § 1.º e § 2.º, da mesma LGPD sobre os mecanismos de limitação de riscos:

Tabela 3 – Comparação entre artigos da LGPD.

LGPD	
Artigo 44	Artigo 50
Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.	Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1.º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, **a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular**. § 2.º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6.º desta Lei, o controlador, **observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados**, poderá: […]

Fonte: Elaboração da autora.

Os riscos esperados e as circunstâncias relevantes impeditivas da caracterização de responsabilidade (artigo 44) devem estar de acordo com o tratamento de dados indicado no artigo 50. Afastando-se da discussão doutrinária sobre a culpa dos agentes de tratamento de dados nas relações de consumo, cabe destacar o caráter objetivo e solidário da responsabilização na LGPD, especialmente entre o controlador[132] e o operador, inclusive na reparação de danos coletivos[133], salvo nas hipóteses de excludentes de responsabilidade caracterizadas no artigo 43 da lei:

> A responsabilização objetiva impõe-se em razão da própria feição dos danos, permitindo a verificação sob condições mais adequadas à espécie e, também, mais céleres. Em igual direção, a responsabilização solidária decorreu da necessidade da apuração das condutas dos diversos atores negociais envolvidos nas redes singulares dos novos pactos e, especialmente, no âmbito do comércio eletrônico (FERREIRA; ROSA, 2019, p. 8).

[132] Para efeitos conceituais, o controlador é o sujeito competente para decisões sobre o tratamento de dados. Já o operador será aquele que efetivamente trata o dado pessoal. O encarregado exerce a função consultiva ou de interface entre o controlador, o operador e a Autoridade Nacional de Proteção de Dados (ANPD) (TASSO, 2020, p. 102). Miragem (2021, p. 488), em termos simples, afirma que o "controlador decide; o operador executa".

[133] Ver o artigo 42 da Lei n.º 13.709/2018.

Nesse aspecto, frisa-se novamente a utilização do CDC como nítida referência para a estipulação de excludentes de responsabilidade configuradas na LGPD.

Tabela 4 – Comparação: CDC *versus* LGPD.

CDC		**LGPD**
Art. 12. […] § 3.º O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que **não colocou o produto no mercado**; II - que, **embora haja colocado o produto no mercado, o defeito inexiste**; III - a **culpa exclusiva do consumidor ou de terceiro**.	Art. 14. […] § 3.º O fornecedor de serviços só não será responsabilizado quando provar: I - que**, tendo prestado o serviço, o defeito inexiste**; II - a **culpa exclusiva do consumidor ou de terceiro**.	Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem: I - que **não realizaram o tratamento de dados pessoais** que lhes é atribuído; II - que, **embora tenham realizado o tratamento de dados pessoais que lhes é atribuído,** não houve violação à legislação de proteção de dados; ou III - que o **dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro**.

Fonte: Elaboração da autora.

Tais excludentes destacadas rompem o nexo causal entre o tratamento e o dano (I e III) e excluem a conduta ilícita do agente (II) (MIRAGEM, 2021, p. 489). No primeiro aspecto, vale ressaltar a solidariedade do fornecedor/agente de tratamento de dados em razão da assunção dos riscos pelos prepostos, empregados e representantes (artigo 34 do CDC) (TEIXEIRA; ARMELIM, 2020, p. 317). No último, é importante frisar o necessário cumprimento dos deveres mencionados nos artigos 6.º e 7.º da LGPD, especialmente quando a base legal do tratamento for o consentimento do titular.

De acordo com a LGPD, o dever de segurança é diretamente imputável aos agentes de tratamento de dados pela própria natureza da sua atividade: “a responsabilidade dos agentes de tratamento decorre do tratamento indevido ou irregular dos dados pessoais do qual resulte dano” (MIRAGEM, 2019a, p. 26). O mesmo ocorre com o fornecedor no CDC. Os riscos inerentes ao desenvolvimento da atividade, tanto do fornecedor no CDC, quanto dos agentes de tratamento de dados na LGPD, estão ligados ao dever de segurança, consideradas as excludentes indicadas em ambas as leis.

Quanto à proteção do consumidor inserido nesse contexto de disposição e de acesso a dados, a LGPD faz clara referência ao CDC ao afirmar que, para as violações de caráter

consumerista, permanecem as regras de responsabilidade estabelecidas no CDC[134], ou seja, responsabilidade objetiva, ressalvadas as excludentes e exceções. Na caracterização do fato do serviço ou defeito – artigo 14 do CDC –, tanto os agentes como os fornecedores são responsáveis solidários pelo tratamento que resulte em dano:

> Incidem tanto as condições de imputação da responsabilidade pelo fato do serviço (em especial o defeito que se caracteriza pelo tratamento indevido de dados, ou seja, desconforme à disciplina legal incidente para a atividade), quanto as causas que porventura possam excluir eventual responsabilidade do fornecedor (artigo 14, §), que estão, porém, em simetria com o disposto no próprio artigo 43 da LGPD (MIRAGEM, 2019a, p. 27).

Em caso de responsabilização, serão levados em consideração os seguintes critérios para a valoração do dano:

> a) a quantidade de dados pessoais afetados;
> b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis, por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;
> c) a reincidência da conduta;
> d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;
> e) a ausência de notificação dos usuários da ocorrência do incidente;
> f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros (CAPANEMA, 2020, p. 168).

É importante destacar a admissão de inversão do ônus da prova em ambas as leis em caso de caracterização de verossimilhança da alegação ou quando o consumidor for hipossuficiente e, considerando a parte final do § 2.º do artigo 42 da LGPD, quando a produção da prova for excessivamente onerosa para o titular dos dados.

Por outro lado, a LGPD também admite a responsabilização administrativa imposta pela ANPD[135]. Conforme o artigo 52 da LGPD, a ANPD possui poder para aplicar sanções ligadas ao tratamento de dados e ao exercício da atividade dos agentes controladores. O artigo 53 da mesma lei estabelece que a ANPD regulará os procedimentos para a imposição de penalidades administrativas, em observância ao direito à ampla defesa e ao contraditório.

A LGPD apresenta uma dubiedade na configuração da obrigação legal dos agentes de tratamento de dados – de meio ou de resultado. Considerando o princípio da responsabilidade e da prestação de contas (*accountability*), devem ser adotadas medidas eficazes no tratamento

---

[134] Ver o artigo 45 da Lei n.º 13.709/2018.

[135] Uma das maiores críticas à Lei n.º 13.709/2018 recaiu no veto ao artigo 55, cuja principal implicância foi a retirada da ANPD, cujo papel principal era a fiscalização e a elaboração de diretrizes para a instauração da Política Nacional de Proteção de Dados. Como argumento justificador do veto, foi indicado vício na iniciativa, uma vez que a criação da entidade vinculada ao Ministério da Justiça incidia apenas no Executivo. É fato que tal veto representou a inequívoca incerteza sobre a efetividade da aplicação da lei pelo recorte da autoridade de fiscalização. Nesse sentido, pelo vasto clamor social e pelas inexoráveis críticas, a Presidência da República, em 27 de dezembro de 2018, criou, por meio de MP 869, a ANPD, aprovada em maio de 2019 pela Câmara e pelo Senado, e sancionada em julho de 2019 pelo presidente da República por meio da Lei n.º 13.853/2019.

de dados[136] com comprovado atendimento aos preceitos legais, o que configuraria a obrigação de resultado. No entanto, a própria legislação estipula normas de conduta nos seus artigos 46 e 50, vinculando, assim, a obrigação de meio (BIONI; DIAS, 2020, p. 19-20). Independentemente do entendimento sobre essa questão, no tratamento de dados de consumo, entende-se pelo afastamento da culpa, em observância inclusive ao disposto no artigo 14, § 4.º, do CDC, sendo aplicada a responsabilidade objetiva à incidência de dano.

Por fim, nas reparações de danos consumeristas, é necessário atentar para o prazo prescricional previsto no artigo 27 do CDC – cinco anos, a contar do conhecimento do dano ou da sua autoria.

4.3.3 Tutela coletiva na proteção de dados de consumo

O microssistema processual coletivo evidencia o policentrismo e tem por base a harmonização sistemática entre várias leis. É um diálogo das fontes: Constituição Federal, Código de Processo Civil, Código de Defesa do Consumidor, Lei de Ação Popular, Ação Civil Pública, Lei de Improbidade Administrativa, Lei de Mandado de Segurança e demais leis avulsas (DIDIER JR.; ZANETI JR., 2017, p. 51-54), além da mais nova LGPD.

A Lei da Ação Popular (Lei n.º 4.717/1965) foi a primeira norma a destinar uma tutela específica aos direitos coletivos. Quase 20 anos depois, com a Lei n.º 7.347/1985 – Lei da Ação Civil Pública –, o ordenamento jurídico brasileiro avançou graças à criação de uma ação judicial específica para a defesa de direitos metaindividuais (difusos e coletivos) (ZAVASCKI, 2007, p. 37-38). A Lei da Ação Civil Pública foi alterada pela Lei n.º 8.884/1994 – Lei Antitruste –, que possibilitou a repressão do dano moral na esfera coletiva. A Lei n.º 8.429/1992 – Lei de Improbidade Administrativa – também abarca direitos eminentemente coletivos.

A Lei de Ação Civil Pública disciplina a ação de responsabilidade por danos causados ao meio ambiente e aos consumidores pelo prisma coletivo, além de mais grupos especificados. O CDC (Lei n.º 8.078/1990) ampliou o conceito de consumidor ao equipará-lo à coletividade, no artigo 2.º, parágrafo único, e no artigo 29. Assim, o CDC inseriu o consumidor nos direitos difusos, coletivos (sentido estrito) e individuais homogêneos.

---

[136] LGPD: "Art. 6.º [...] X. responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

O interesse difuso é aquele que não permite a identificação de seus sujeitos titulares, que são indeterminados e não permitem o fracionamento do objeto. Como exemplo da manifestação da tutela difusa, pode-se citar a oferta e a publicidade (arts. 30 a 38 do CDC). Conforme os artigos 81 e 82 do CDC, qualquer legitimado extraordinário é competente para a defesa, independentemente do fato de o consumidor sentir-se prejudicado. Os interesses difusos são abstratos, indeterminados, indivisíveis e internamente litigiosos (VERBICARO, 2017).

O direito coletivo em sentido estrito surge no artigo 129, III, da CF. Representa a síntese dos interesses de um grupo, passíveis de identificação quanto à apuração do dano e da responsabilidade. Haverá o reconhecimento de uma relação jurídica de base, ou seja, uma limitação natural ao alcance da tutela. Portanto, a principal distinção entre interesses difusos e coletivos em sentido estrito é a determinabilidade dos sujeitos (VERBICARO, 2017).

Os interesses individuais homogêneos constituem uma inovação jurídica do CDC, nos artigos 91 a 93. Na sua essência, são individuais, podendo ser coletivizados pela instrumentalização pela via coletiva e por meio do legitimado extraordinário. Para Verbicaro (2017), a coletivização de um interesse que, originalmente, era meramente individual subjetivo trará vantagens ao consumidor, uma vez que a pluralidade de consumidores lesados terá melhores condições de influir de modo decisivo na própria convicção do magistrado.

Segundo Cohen (2013, p. 1909), a privacidade não é uma condição fixa, uma vez que está diretamente vinculada à relação individual com o social dinâmico. Para a autora, o objetivo da privacidade é garantir o desenvolvimento subjetivo e comunitário sem colisão (COHEN, 2013, p. 1911).

Para Leonardi (2012, p. 232), em uma sociedade de massa, os mecanismos de tutela individual resolvem as pretensões isoladas levadas a juízo, mas “dificilmente levam a mudanças concretas nas práticas de mercado e modelos de negócio adotados por empresas”. No que diz respeito à proteção da privacidade no ciberespaço, a defesa coletiva da privacidade quanto ao acesso, tratamento e disposição de dados pessoais é o mecanismo mais eficaz para buscar o objeto tutelado. No mesmo sentido, Mantelero (2016 *apud* ZANATTA; SOUZA, 2019, p. 396) afirma:

> As análises investigam atitudes e o comportamento de grandes grupos, comunidades e até países inteiros. Além disso, essas novas formas de análise não investigam necessariamente grupos pré-existentes. Grupos são criados por coletores de dados que selecionam conjuntos específicos de informações [...]. Esse cenário torna necessário considerar um campo de análise mais amplo, representado pelos interesses difusos dos indivíduos que possuem seus dados pessoais coletados, analisados e agrupados em grupos e categorias.

Como caso concreto, pode-se citar:

> A empresa Google Brasil Internet recusava-se terminantemente a fornecer dados cadastrais e de conexão capazes de auxiliar na identificação de autores de atos ilícitos cometidos por meio de seus serviços, sob o argumento de que essas informações estariam localizadas em servidores nos Estados (todos são considerados consumidores dos serviços, por exemplo), que gozam de um direito coletivo, tutelável por meio de um provimento jurisdicional uniforme, de forma a cessar eventuais práticas ilícitas que afetem todos eles, de modo indivisível. Unidos, sob controle de sua matriz, Google Inc., muitas ações individuais foram promovidas por vítimas de atos ilícitos com esse mesmo objetivo, sem obter sucesso. Diversos pedidos similares do Ministério Público Federal, em ações penais individuais, foram igualmente rejeitados. O problema apenas foi resolvido após a propositura de ação civil pública pelo Ministério Público Federal, cujo escopo era obrigar a empresa a fornecer esses dados, sob pena de multa diária e, em último caso, de dissolução compulsória da empresa, bem como obter sua condenação ao pagamento de indenização, a título de dano moral coletivo (LEONARDI, 2012, p. 235-236).

Para Leonardi (2012), as maiores dificuldades para a eficácia da tutela coletiva são: a) as amarras criadas pela Lei n.º 9.494/1997, as quais pretenderam limitar os efeitos da coisa julgada nas ações coletivas ao território da competência da ação – a limitação pode tornar-se absurda se considerada a desterritorialidade do ambiente virtual; b) a necessidade de maior participação de entidades civis na tutela coletiva, algo que não tem ocorrido na prática forense. Verbicaro e Costa (2018) confirmaram a segunda dificuldade em uma pesquisa empírica realizada nos processos físicos no Fórum Cível da Comarca de Belém: encontraram apenas três processos ajuizados por associações representativas de defesa do consumidor, ressaltando que uma única associação teria sede no Estado do Pará, o que demonstra a total inatividade da representação. Ainda no âmbito extraprocessual, sobre a atuação das associações civis, constataram:

> Apesar de o número ser considerado pequeno, o que poderia ser compensado por meio da atuação ativa dessas associações, a informação prestada pela Gerência de Educação e Projetos do órgão administrativo adverte que a atuação destas se restringe apenas a participação – de indivíduos que se intitulam como representante – em eventos organizados pelo PROCON, não havendo registro de representações, denúncias ou solicitação de parcerias de quaisquer associações (VERBICARO; COSTA, 2018, p. 79).

Leonardi (2012, p. 245) afirma ser possível "exigir que determinado *Web site* ou rede social modifique sua arquitetura para assegurar a proteção da privacidade de seus usuários, de modo a deixar de coletar, automaticamente, dados pessoais". No entanto, o mecanismo para implementar mudanças permanentes na arquitetura dos serviços é a tutela coletiva, uma vez que a individual poderá, sim, reparar o interesse subjetivo da vítima, mas dificilmente ensejará mudanças sociais.

A LGPD adotou uma perspectiva coletivista para a proteção dos dados pessoais, como "a avaliação do impacto à comunidade, a proteção dos nossos direitos fundamentais e a reparação coletiva por violações éticas e aos valores da sociedade" (ZANATTA, 2019, p. 202). Conforme se viu na subseção 3.2, para Rodotà (2008), a proteção da privacidade vai além de

uma proteção de caráter individualista personalíssimo; reside na tutela coletiva contra os impactos causados por uso indevido de dados pessoais.

Segundo Zanatta (2019, p. 202-205), a coletivização da proteção de dados de consumo tem cinco elementos-chave: a) a crescente importância dos direitos coletivos e difusos sob a perspectiva da violação da própria sociedade; b) a possibilidade de proteção dos dados por entidades civis; c) a proteção do ambiente informacional em uma perspectiva preventiva, com base no princípio da precaução e da segurança; d) a redefinição da estrutura administrativa de defesa do consumidor; e) a atuação repressiva do Ministério Público[137].

São nítidas a complementaridade e a conexão entre a LGPD e o CDC na tutela coletiva. Assim, o artigo 22 da LGPD estabelece que a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual e coletivamente. O artigo 42, *caput*, da LGPD faz menção ao fato de que a violação da legislação de proteção de dados pessoais pode acarretar danos patrimoniais ou morais, inclusive coletivos. Por fim, o § 3.º do mesmo artigo diz que as ações de reparação por danos coletivos decorrentes da violação da proteção de dados pessoais podem ser exercidas coletivamente em juízo, incidindo subsidiariamente a legislação específica, como a Lei n.º 7.347/1985, os artigos 81 a 104 do CDC, a Lei n.º 4.717/1965 (Ação Popular) e os artigos 21 e 22 da Lei n.º 12.016/2009 (ROQUE, 2019).

Conforme Roque (2019, p. 16), é absolutamente necessário aprofundar o estudo da tutela coletiva de dados pessoais:

> (i) a proteção de dados pessoais na esfera coletiva pode dar origem a direitos difusos, coletivos em sentido estrito ou individuais homogêneos; (ii) são legitimados coletivos para a proteção de dados pessoais todos aqueles relacionados no art. 5.º da Lei n.º 7.347/1985 e no art. 82 do CDC, sem prejuízo da legitimação do indivíduo, em situações excepcionais; e (iii) deve-se admitir a formulação de pedido genérico de reforma estrutural, na forma do art. 324, § 1.º, do CPC, havendo fundamento legal para a adoção das medidas estruturantes, sobretudo na fase de cumprimento de sentença, nos arts. 139, IV, e 536, § 1.º, do CPC.

Zanatta e Souza (2019, p. 410) frisam que a tutela coletiva busca não somente perseguir o dano, mas também tutelar "na forma específica os eventuais ilícitos que estejam sendo cometidos" – uma tutela inibitória em caso de provada ameaça ao direito.

A leitura do artigo 22 junto com o artigo 42 da LGPD, em diálogo com o CDC, permitirá a atuação repressiva e preventiva das autoridades administrativas – Secretaria Nacional do Consumidor (Senacon) e ANPD – e judiciárias para assegurar a tutela coletiva da proteção de dados pessoais (ZANATTA; SOUZA, 2019, p. 412). É importante frisar que a atuação

[137] "Desde a criação da Comissão Especial de Proteção de Dados Pessoais no Ministério Público do Distrito Federal e Territórios (MPDFT), dezenas de inquéritos foram instaurados contra empresas que supostamente violaram as regras da LGPD, antecipando o *enforcement* da legislação" (ZANATA, 2019, p. 205).

preventiva deve garantir o consentimento ativo das categorias inseridas no contexto discutido, bem como observar as formas de responsabilização nos casos em que a permissão ao tratamento de dados for eivada de vícios. A proteção do legítimo consentimento, quando for a base legal do tratamento de dados, além da proteção de qualquer tipo de dano, deve impedir o estado de danosidade permanente do consumidor, individual ou coletivo, no mercado informacional.

4.4 Consentimento e responsabilidade civil: entre o dano e o estado de danosidade social

O corolário do tratamento de dados pessoais é o exercício da autodeterminação informativa, seja pela possibilidade de oposição, bem como do consentimento ativo e legítimo, seja por hipótese legal autorizativa diversa.

A LGPD e o CDC, em nítido diálogo entre fontes, estabelecem regras claras para efetivar a transparência relacional no intuito de diminuir as vulnerabilidades atinentes à relação de consumo de dados, assentando na imposição do devido processo informacional:

> [...] é possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais a preservação de verdadeiro "devido processo informacional" (*informational due process privacy right*), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios[138].

Bioni (2020b, p. 4) aduz que "alguns dos principais problemas encontrados com sistemas de tomada de decisão automatizada incluem: falta de transparência, dificuldade de identificação e correção de erros, dificuldade de contestar decisões e reforço de desigualdades já existentes".

A prevenção de danos relativos à relação de consumo é indissociável da informação do consumidor (FONSECA, 2019, p. 168). Com base no diálogo entre o CDC e a LGPD, pode-se dizer que a inobservância de regras técnicas na realização do consentimento verdadeiramente ativo expõe o consumidor a um estado de danosidade no mercado informacional.

Para Fonseca (2019, p. 142), o dano está relacionado à necessária diminuição ou à destruição de um bem jurídico, patrimonial ou moral. O estado de danosidade abarca o conceito de dano. Trata-se de evitar ou de prevenir o dano concreto, tendo como fundamento a prevenção ou a precaução.

> A razão de defedermos a ampliação conceitual do dano (e não do risco), em uma verdadeira travessia do dano para danosidade, assenta-se na força normativa de

[138] STF (Plenário). ADI 6389/DF. Relatora: Min. Rosa Weber. Data do julgamento: 17/11/2020. Data da publicação: 30/11/2020. p. 108.

> prevenção, que requer que os agentes atentem para a potencialidade dos danos, cumprindo deveres de prevenção, com adoção de medidas necessárias para isto, o que mitiga a "certeza" do dano como requisito que se configure a obrigação de indenizar (FONSECA, 2019, p. 147).

O essencial não é evitar o dano concreto e imediato, é evitar lesões ou interferências injustas na espera jurídica, individual e coletiva (FONSECA, 2019, p. 153). Os agentes de tratamento de dados têm o dever de evitar que se forme o estado de danosidade, tendo em vista a prevenção, pautada pelos princípios da precaução e da segurança. Afirma Fonseca (2019, p. 157):

> Portanto, o responsável deve passar a ser não apenas aquele que causou o dano concreto, mas, também, aquele que tinha o dever jurídico de evitá-lo, de modo que a conduta ilícita não se liga ao dano efetivo, mas à esfera jurídica do indivíduo afetado seja pelo desprezo do ofensor pelas normas protetivas, ou pelo incremento injusto dos riscos, ou ainda, pela ausência de medidas de prevenção ao dano. Tais situações inserem o indivíduo em um estado injusto potencialidade de dano concreto.

O consumidor, individual ou coletivo, no mercado informacional está exposto ao risco de um tratamento de dados que não observa as técnicas de prevenção de dano. Por isso, o artigo 4.º, V, do CDC incentiva a "criação pelos fornecedores de meios eficientes de controle de qualidade e segurança de produtos e serviços".

Para Verbicaro (2017, p. 237), o consumidor exposto ao dano potencial por prática irregular autoriza a imputação de responsabilidade. Expor, portanto, o consumidor a um vício de consentimento provoca um estado de danosidade. Quando se analisa o consumidor coletivo em face de uma condição de danosidade, observa-se que é necessário proteger não somente uma categoria, mas o próprio interesse público.

Nos processos de caráter coletivo, a concepção construtivista da relação entre direito e sociedade vai além das decisões judiciais, gerando transformações sociais. De fato, há decisões que não somente provocam mudanças na conduta dos indivíduos diretamente envolvidos no caso, mas também produzem transformações indiretas na sociedade (RODRÍGUEZ-GARAVITO, 2011). Portanto, trata-se de litígios de interesse público em razão da projeção coletiva, fática e jurídica da demanda.

Para Salles (2003, p. 40-41), a expressão "interesse público" designa o interesse da generalidade das pessoas que buscam a máxima efetividade dos objetivos sociais. Para Didier Jr. e Zaneti Jr. (2017, p. 39), o interesse público pode ser primário – o conjunto de interesses coletivos – e secundário – voltado para a satisfação do interesse da administração pública. A tutela coletiva visa a satisfação do interesse público primário.

Para Theodoro Júnior, Nunes e Bahia (2013, p. 136), é necessário somar estratégias além da judicialização, para que o Estado garanta efetividade aos direitos por meio da adoção

de medidas adequadas, progressivamente, segundo os recursos disponíveis, com base no princípio da razoabilidade.

A LGPD e o CDC, portanto, por meio da prevenção e da segurança, buscam impedir a ocorrência de riscos. Para isso, é necessário o compartilhamento da autoridade política entre o Estado, o consumidor e o fornecedor da relação. Apesar da importância assumida pela responsabilização por uso indevido de dados pessoais, medidas preventivas devem ser tomadas a fim de evitar o estabelecimento do estado de danosidade do consumidor.

5 A CIDADANIA INSTRUMENTAL NA PROTEÇÃO DOS DADOS DOS CONSUMIDORES: O COMPARTILHAMENTO DA AUTORIDADE ENTRE OS AGENTES DA RELAÇÃO

A solidariedade emancipatória é a base do rompimento das promessas descumpridas da modernidade. Tal afirmação é a principal premissa para o estabelecimento do compartilhamento da autoridade nas relações de consumo tendo em vista o exercício da cidadania instrumental na relação de proteção de dados de consumo.

A sociedade indolente, competitiva, individualista, cuja liberdade negativa é exaltada e fonte ensejadora do direito, causa uma falsa sensação de segurança, uma vez que, embora o Estado seja visto como garantidor de direitos, exsurgem políticas desiguais, que fragilizam mais ainda o vulnerável da relação:

> Um Estado liberal e abstencionista não reconhece, nitidamente, todas as categorias sociais, principalmente aquelas com maior nível de debilidade econômica, como por exemplo: os trabalhadores, os idosos, os portadores de necessidades especiais, tampouco o consumidor, objeto de análise. Como também dependem das pretensas virtudes da representação política e como essa habitualmente despreza a minoria, as categorias acima ficarão à margem de um reconhecimento mínimo quanto à sua expressão e direitos, mas muitas vezes, por também se iludirem em relação à sua pseudoigualdade propagada, não percebem tal distorção no modelo democrático, muito menos se sentem impelidos a exigir mudanças (VERBICARO, 2017, p. 52).

Não se pretende desconsiderar a proteção de liberdades negativas (VERBICARO, 2017, p. 53). Mas defende-se o reconhecimento de lacunas na busca de alternativas conjuntas para a proteção coletiva dos consumidores e, por conseguinte, o estabelecimento de direitos positivos essencialmente necessários quando se analisa o concreto dever de autodeterminar suas informações na economia informacional, ora analisada.

Na modernidade, há duas maneiras de conhecer o mundo e de nele atuar – os denominados paradigmas epistemológicos e sociais (SANTOS, 2002, p. 75): o conhecimento-regulação e o conhecimento-emancipação. Verbicaro (2017, p. 24-99) explica os dois tipos de conhecimento: o conhecimento-regulação é aquele em que o ponto de ignorância é o caos e o ponto de conhecimento é a ordem; já o conhecimento-emancipação é aquele em que o ponto de ignorância é o colonialismo e o ponto de conhecimento é a solidariedade.

O conhecimento-regulação favoreceu o fortalecimento do Estado, como principal garantidor de direitos, e do mercado, a sua força predatória, especialmente no exercício da sua soberania mercadológica[139] O desafio é a reinvenção por meio da transição paradigmática do

[139] O capitalismo desqualifica a política. O Estado muda as suas funções com o seu desenvolvimento. Conforme Harvey (2005), a ascensão do capitalismo foi acompanhada da criação e da transformação das instituições e das

conhecimento-regulação ao conhecimento-emancipação, em que o Estado reconhece suas limitações e a própria sociedade, com uma participação ativa, privilegia a ideia de solidariedade como a própria emancipação cívica:

> [...] a solidariedade, como caminho da emancipação, procura traduzir e satisfazer as promessas e expectativas que a experiência da racionalidade não foi capaz de produzir. O Direito, nesse contexto, é visto sob uma nova temática, ou seja, sob uma nova perspectiva crítica através da rediscussão da origem, fonte, fundamento, alcance e eficácia da norma jurídica (VERBICARO, 2017, p. 48).

A solidariedade defendida não se limita ao conceito de conduta beneficente ou de ajuda assistencial, mas implica uma mudança de consciência moral (VERBICARO, 2017, p. 67). A sociedade redescobre o seu papel e vê-se por um prisma coletivo, mesmo que obtido por enxame ou por uma solidariedade mecânica (BAUMAN, 2008, p. 57). Esse contexto exige uma alteração estatal e no direito em si que "passa a valorizar a solidariedade, abandonando o individualismo jurídico, tornando-se um fenômeno mais plural, alicerçado em uma fundamentação ética capaz de produzir equilíbrio social" (VERBICARO, 2017, p. 75).

Assim, há um inexorável convite a descentralização do poder: de um lado, uma sociedade dialogante, deliberante e, acima de tudo participativa, o Estado e o Direito assumem uma postura democrática; de outro, o mercado reconhece direitos das categorias vulneráveis que necessitam de tratamento específico, desde a concepção do produto e serviço. Essa descentralização suscitará o compartilhamento da autoridade política pelo compromisso tripartido na relação.

O direito do consumidor é a expressão do ideal de solidariedade. O CDC privilegia o pluralismo jurídico ao criar novos espaços políticos de deliberação, por meio da Política Nacional das Relações de Consumo (PNRC) (VERBICARO, 2018), o que relativiza as fontes estatais, fortalece a tutela de interesses transindividuais e o compartilhamento da autoridade política. O Estado passa a ser o mediador entre os interesses do mercado e os do consumidor (VERBICARO; VIEIRA, 2020b):

> A Política Nacional das Relações de Consumo prevista nos artigos 4.º e 5.º do CDC (LGL\1990\40) foi desenhada como um compromisso tripartido entre o Estado, a sociedade civil e o empresário, promovendo não apenas um compartilhamento de poder do Estado, mas também buscando incentivar o resgate da autoestima cívica do grupo, que se vê como categoria de consumidores, possuindo melhores instrumentos para a defesa de seus interesses (VERBICARO, 2017, p. 19).

Tal política deliberativa influirá no sentimento de pertencimento e de atuação conjunta, o que "forjará o novo conceito de cidadania instrumental para as relações de consumo"

---

funções estatais para satisfazer às necessidades específicas do capital. Nesse sentido, o Estado capitalista precisa desempenhar suas funções básicas para o desenvolvimento do capital, caso contrário, deverá ser reformado ou dar lugar a outro método de organização da produção material e da vida cotidiana. Ver Vieira (2019).

(VERBICARO, 2017, p. 3). O estabelecimento dessa cidadania, de forma coletiva, em atenção, inclusive, à proteção transindividual estabelecida do CDC, a participação do Estado como árbitro de interesses divergentes e o comportamento ético das empresas, na busca da realização de uma relação preventiva e de confiança, exigirão a harmonia na relação:

> Essa arquitetura institucional, inerente aos novos espaços políticos de participação, deverá estar em sintonia com os postulados da transição paradigmática em direção à solidariedade, donde se percebe um círculo virtuoso no modelo emancipatório, pois quanto maior o grau de envolvimento do consumidor no contexto decisório, melhores serão os resultados e mais consistentes as mudanças, o que gerará mais confiança, aguçando o sentimento de empatia ou pertença ao grupo, tudo isso multiplicado sucessivamente (VERBICARO, 2017, p. 17).

O equilíbrio na relação em discussão, portanto, requer práticas responsáveis dos três agentes. A sociedade deve desvincular-se de práticas indolentes e individualistas para buscar a defesa de seus direitos de maneira transindividual, seja pela tutela coletiva judicial, seja pela tutela extrajudicial por meio do empoderamento do consumidor.

O Estado deixa de ser o principal componente e impositor de direitos para ser o mediador dos interesses sociais e mercadológicos, incentivando políticas voltadas para a educação para o consumo, a participação ativa da sociedade, o estabelecimento de práticas de segurança, de caráter fiscalizatório ou punitivo, e, ainda, uma arquitetura de rede preventiva, englobando, assim, políticas de governabilidade que afetam diretamente os fornecedores. Nesse aspecto, é importante destacar a função da ANPD e o desenvolvimento da Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPDPP), conforme será visto adiante.

Segundo Zak (2012, p. 159), se se reconhece o mercado como um contrato social, é preciso implantar políticas que correlacionem o comportamento moral, a eficiência e a lucratividade nas transações, mesclando o interesse individual com o bem social, a construção da confiança e, consequentemente, a fidelização do consumidor. É preciso ainda impor as práticas preventivas de segurança dispostas na LGPD, como o *compliance* e o PbD (5.3), bem como promover uma atuação conjunta dos agentes, pautada pelo princípio da prevenção e do princípio da prestação de contas – *accountability* – presentes na estrutura legislativa brasileira.

5.1 O consumidor e o seu empoderamento no ambiente virtual

A tecnologia, a digitação (automação) e a informação representam uma ruptura e implicam mudanças significativas em todos os aspectos da vida. Nas relações de consumo, essa revolução tornou possível a existência de novos produtos e serviços (SCHWAB, 2018, p. 20). Os consumidores estão redefinindo experiências e abordagens tradicionais sobre segmentação

demográfica, adotando critérios digitais, como a identificação baseada em dados (SCHWAB**,** 2018, p. 58-59).

Trata-se de um novo paradigma de comportamentos que intervém diretamente nos meios de produção e nas relações de consumo, com duas fontes comportamentais: a primeira está relacionada com a modulação comportamental por meio do processamento de dados; a segunda vincula-se à maior transparência e participação ativa na avaliação de desempenho das empresas e, assim, ao fortalecimento cívico no ambiente virtual[140]:

> Vale destaque ao fato de que o consumidor digital busca as informações e relatos de experiências nas mídias sociais por duas motivações, o fácil acesso à internet e a ausência de interação e escassez de informações pelo próprio fornecedor quanto ao bem que será consumido. Logo, não raras vezes, há a possibilidade de o consumidor em potencial procurar referenciais através de publicidades, sites de reviews, canais do Youtube, opiniões de digitais influencers para firmar sua convicção acerca da compra que deseja realizar (FREIRE, 2020, p. 150).

O empoderamento do consumidor é atualmente o principal influenciador de práticas responsáveis nas empresas. As empresas entendem que a análise do perfil do consumidor será uma excelente matéria-prima para o direcionamento publicitário, bem como o monitoramento do grau da (in)satisfação dos clientes.

O uso da internet reconfigurou o exercício do consumo e a própria caracterização do consumidor. O "consumidor 4.0" expressa o seu poder decisório sobre os interesses de práticas comerciais. Tal mudança no perfil comportamental exprime características específicas, como maior exigência em suas escolhas, conexão em rede, comodidade e instantaneidade (COSTA; OLIVEIRA; LEPRE, 2020, p. 505-507). No entanto, é importante ressaltar que essa reconfiguração é limitada, uma vez que a inclusão tecnocívica não é qualitativa, dadas as vulnerabilidades existentes no contexto estudado, o que gera exclusões e isolamento (LIMBERGER; SALDANHA; HORN, 2017).

O ambiente virtual aumentou o grau de solidariedade mecânica entre os consumidores na defesa de interesses específicos. A dinâmica desenvolvida na rede coletiva é aberta e o acesso é livre, o que pode ampliar a visibilidade, as indagações e as controvérsias sobre o assunto discutido. É mister destacar que a noção de empoderamento não se limita à abordagem comunicativa em rede, reflete-se também nas inquietudes em relação à marca do fornecedor (FREIRE, 2020, p. 152).

---

[140] "A internet é marcada desde seu início pela interferência de seus usuários, por parte de expressão de suas opiniões, manifestações e, sobretudo, pela composição constante de novos conteúdos, bem como pela reconfiguração dos já existentes. Até aqui tivemos meios de comunicação que eram dirigidos para a audiência. Agora com a internet, temos uma mídia na qual a audiência tem participação efetiva e marcante como autora, promotora e detentora de conteúdos" (BORGES, 2017, p. 118).

O consumidor, ao reconhecer a sua vulnerabilidade relacional, busca, por meio de informações, modos alternativos para solucionar o problema (SOLOMON, 2011). Em outros termos, o consumidor tem tomado consciência de seu poder decisório por meio da escalabilidade, do uso de marca, da customização empresarial e da reconfiguração identitária nas mídias sociais (FREIRE, 2020, p. 147-148):

> O empoderamento virtual do consumidor e mesmo a técnica de "cancelamento mercadológico", também denominado de boicote tem produzido mudanças sensíveis nesse novo espaço de interação econômica entre os sujeitos da relação de consumo e, o que é melhor, decorrem da mobilização espontânea e dinâmica da sociedade de consumidores e de forma independente à atuação dos órgãos governamentais, com respostas muito mais rápidas e efetivas (VERBICARO; OHANA; VIEIRA, 2020, p. 54).

Para Longo (2014), as empresas beneficiam-se da vulnerabilidade informacional da relação de consumo. Em contrapartida, os consumidores optam cada vez mais pela interação como mecanismo de combate a práticas predatórias das empresas:

> [...] é possível observar que contaram o ocorrido para todos os seus amigos e familiares para protegê-los de futuras frustrações (80%); entraram em contato com a empresa e registraram a reclamação (79%); e decidiram não se relacionar mais com a empresa/marca (59%), priorizando o registro de suas insatisfações na internet (48,25%) a se direcionar a um órgão de proteção do consumidor para registro do problema (34,01%), dentre estes, 11,3% realizaram a reclamação a um PROCON (COSTA; GONÇALVES; MOTA, 2016, p. 36).

Portanto, os consumidores digitais buscam em outros consumidores informações para analisar a qualidade do produto ou serviço, o que exigirá das empresas uma maior preocupação com a satisfação do cliente, uma vez que esse sujeito será o seu maior refutador ou vendedor. Freire (2020, p. 149) confirma tal fato:

> [...] ao empoderamento público e à postura de cidadão que têm sido cada vez mais assumidos na sociedade pelos consumidores, com intuito de transformar o processo comunicacional unidirecional – foco de oitiva apenas na empresa – em multidirecional – foco compartilhado com o consumidor e potenciais consumidores, almejando maior simetria e paridade entre as organizações, clientes e demais stakeholders […].

Tal empoderamento virtual, também conhecido como ativismo identitário[141], visa difundir uma imagem negativa do fornecedor, punindo-o socialmente em razão da realização de condutas eticamente irresponsáveis. Por conseguinte, busca modificar condutas empresariais desterritorializadas a fim de alcançar o equilíbrio mercadológico.

O exercício da liberdade, por meio do empoderamento, provoca mudança nas práticas comerciais. Para Freire (2020, p. 184), "aos poucos, identidades de usuários que, ainda de modo

[141] Borges (2017, p. 125-132) utiliza o termo "net-ativismo" para designar o ciberativismo, que apresenta três características: tecnológico informativo, conectivo e reticular (não linear e imprevisível). O autor cita o cancelamento virtual realizado no caso Maria Filó, marca conceituada no mundo da moda que estampou em uma peça de uma nova coleção desenhos de escravas negras servindo mulheres brancas, o que foi denunciado como um ato racista. Sobre o caso Maria Filó, consultar https://catracalivre.com.br/cidadania/colecao-da-maria-filo-usa-estampa-de-escravos-e-causa-revolta/.

individual, quando compartilhados, agregam-se de modo coletivo e tornam possível o ideal de uma inteligência coletiva em defesa de uma maioria ou minoria parcialmente representada". Consequentemente, os atos individuais do consumidor virtual, cidadão essencialmente social, afetam a coletividade, uma vez que o ato de consumir insere-se em toda uma cadeia produtiva. Assim, a insatisfação de um único consumidor, destinatário final, atinge consumidores difusos e potenciais ligados em rede.

As escolhas são "enfatizadas em virtudes cívicas de caráter obrigacional negativo, como as manifestações de boicotes em mídias sociais" (FREIRE, 2020, p. 183), transformando a democracia representativa em participativa por meio do compartilhamento da autoridade política pela solidariedade. Dessa solidariedade entre estranhos e da discricionariedade coletiva (VERBICARO, 2017) surge uma nova dimensão da consciência e da liberdade individual, que incide na restruturação coletiva.

O empoderamento do consumidor deve expressar o exercício da cidadania participativa em consonância com a legislação brasileira e os valores éticos. É preciso proporcionar aos grupos meios de participação ampla, não limitada, a fim de incentivar o diálogo entre as diversas categorias de consumidores (LIMBERGER; SALDANHA; HORN, 2017). Mas a real inclusão qualitativa das partes exige uma articulação de políticas, que visem especialmente a educação para o consumo. O Estado tem um papel essencial na construção de um contexto social, onde a linguagem e a comunicação estão presentes. Não se pode negar o empoderamento do consumidor nem a identificação do consumo identitário como estratégias de enfrentamento das práticas predatórias dos fornecedores na internet. Do mesmo modo, é inegável a necessidade de uma educação transversal (LIMBERGER; SALDANHA; HORN, 2017) no sentido de garantir uma comunicação positiva, evitando a exclusão de categorias de consumidores e o consequente agravamento de suas vulnerabilidades.

5.1.1 O paradoxo entre o consumidor de vidro e o consumidor identitário no contexto pandêmico

Durante a pandemia de Covid-19, destacaram-se duas figuras de consumidores: o consumidor de vidro e o consumidor identitário. Ambos podem estar presentes ao mesmo tempo e contexto, apesar da aparente contradição.

O consumidor de vidro é aquele que se expõe, suas informações são obtidas facilmente pela coleta, pelo tratamento e pelo uso de dados pessoais: "as propriedades e as capacidades do vidro – fragilidade, transparência, capacidade de distorcer o olhar do observador – espelham a

nossa vulnerabilidade" (LACE, 2004, p. 7, tradução nossa)[142]. O consumidor de vidro é constantemente persuadido pelo assédio de consumo porque seu próprio eu é convertido em informações, sendo a publicidade direcionada para a modulação comportamental (VIEIRA; OHANA, 2020).

O consumidor identitário é aquele que exerce o seu empoderamento por meio do consumo vinculado a uma ideologia, ele recorre a um conjunto de elementos valorativos, "evidenciado cada vez mais na mudança de comportamento interativo com o fornecedor, no compartilhamento de experiências/reviews/feedbacks online e até mesmo no ato de incitar boicote às empresas" (VIEIRA; OHANA, 2020).

Ao mesmo tempo que se agravou a vulnerabilidade do consumidor inserido no mercado informacional em razão das assimetrias relacionais estudadas (subseção 3.1), intensificadas pela condição de isolamento, pelo consequente fortalecimento do consumo digital e pela utilização de plataformas de compartilhamento, o consumidor viu-se no centro da interatividade no trato de valores sociais.

Como exemplo, pode-se citar o aumento da coleta de dados pessoais em âmbito mundial para políticas de agregação no combate da pandemia. Por outro lado, grandes atos de boicote impossibilitaram ações predatórias de empresas, como, por exemplo, a venda de máscaras por um preço exorbitante pela Osklen Brasil. A ação dos consumidores não só prejudicou a ação comercial da empresa, como exigiu a sua retração.

De igual forma, o lançamento da marca Vir.Us impactou negativamente o público. Além da crítica ao preço dos produtos, o nome foi considerado "oportunista e infeliz" em relação às vítimas da doença (OLIVEIRA, 2020). A empresa precisou fazer um reposicionamento de mercado, mudando o nome para Amar.Ca. Ações consideradas éticas também foram alavancadas nesse contexto:

> reações positivas dos consumidores em tempos de pandemia puderam ser percebidas como diferenciais para aqueles fornecedores que se demonstravam favoráveis à preservação da saúde de seus funcionários, manutenção dos empregos e doações efetivas para conter os casos de COVID-19, como o caso das empresas Itaú, Magazine Luiza e a Ambev (VIEIRA, OHANA, 2020, p. 454).

Não se pode afirmar que o empoderamento por meio do consumo identitário eliminou ou diminuiu a condição de vulnerabilidade do consumidor. Como se viu no capítulo terceiro, há concretas vulnerabilidades na relação de dados, exacerbadas pela crise pandêmica. No entanto, é fato que a atuação em rede, por meio da solidariedade mecânica, possibilita mudanças

[142] No original: "the properties and the capacities of the glass: fragility, transparency, ability to distort the gaze of the viewer – mirror our vulnerability".

estruturais na relação de consumo. Ainda que lentamente, padrões éticos podem ser estabelecidos pelo temor do fornecedor, que evita uma exposição negativa, e, em outro sentido, pela construção de uma relação de confiança que visa a fidelização do cliente.

5.2 O papel mediador do Estado na proteção de dados de consumo

5.2.1 Autoridade Nacional de Proteção de Dados

Uma das maiores críticas feitas à Lei n.º 13.709/2018 foi o veto ao artigo 55, ou seja, a retirada da ANPD, autoridade administrativa independente responsável pela fiscalização, pela instauração da Política Nacional de Proteção de Dados e pela consultoria aplicada à proteção de dados pessoais. O veto "representou uma inequívoca incerteza sobre a efetividade da aplicação da lei pela supressão da autoridade de fiscalização" (VERBICARO; VIEIRA, 2021a, p. 216).

Em 27 de dezembro de 2018, após inexoráveis críticas, a Presidência da República, por meio da MP n.º 869, estabeleceu a ANPD. Aprovada em maio de 2019 pela Câmara e pelo Senado, foi sancionada em julho de 2019 pelo presidente da República por meio da Lei n.º 13.853/2019.

Em razão da incidência da pandemia Covid-19, novas medidas foram impostas, inclusive à proteção de dados pessoais e à atuação da ANPD. Em 10 de junho de 2020, a Lei n.º 14.010/2020 prorrogou a atuação fiscalizatória para 1.º de agosto de 2021. Em 26 de agosto de 2020, por meio do Decreto n.º 10.474/2020, foi aprovada a estrutura regimental e o quadro dos cargos e funções da ANPD e, consequentemente, do Conselho Nacional de Proteçção de Dados Pessoais e Privacidade (CNPDP).

No mundo, a Carta dos Direitos Fundamentais da União Europeia, de outubro de 2012, foi o primeiro instrumento internacional juridicamente vinculativo a definir, no seu artigo 8.º, uma autoridade independente para estipular regras de prevenção e de controle para a proteção de dados: "O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente" (UNIÃO EUROPEIA, 2012). Os artigos 51 a 59 do Regulamento Geral sobre a Proteção de Dados (UNIÃO EUROPEIA, 2016) apresentam a aplicação dos poderes desse órgão de controle independente, em especial o poder de investigação e de intervenção:

> O poder de investigação, isto é, o direito de acessar os dados que estão sendo tratados e de receber todas as informações necessárias para o pleno desempenho de sua missão de fiscalização e controle; o poder de interdição, entendida como medidas que podem ser adotadas por esta entidade para que a proteção dos dados pessoais seja eficaz, por exemplo, determinar o bloqueio, a destruição de dados, proibir o tratamento de dados

> provisória ou definitivamente etc.; e a capacidade processual para ingressar em juízo quando comprovada uma violação ás regras sobre proteção de dados pessoais (LIMA, 2020, p. 252-253).

Apesar dos entraves políticos e econômicos para a criação e a efetividade de uma ANPD independente, sua implantação fortalece a economia nacional, protege os direitos constitucionalmente protegidos e ainda realiza protege o consumidor inserido no contexto de tratamento de dados no âmbito local e global. No mesmo sentido, Doneda (2019, p. 311-312) destaca:

> Não é exagero identificar a razão de ser desses órgãos, desgarrados da estrutura tradicional e caracterizados pela sua independência, pela especificidade da sua atividade e pelo caráter eminentemente técnico, a uma crescente complexidade das relações sociais e da organização do Estado. Diante dessa necessidade, demonstrou-se necessário que a administração pública se especializasse para atender a cada uma das grandes demandas com o particularismo e a dinâmica necessários. Mais recentemente, verificou-se que diversas características desses órgãos, moldados para responder de forma mais direta e dinâmica a determinadas demandas de natureza econômica, poderiam ser igualmente relevantes no papel da defesa e promoção de direitos do cidadão, proporcionando o surgimento da figura da autoridade de garantia.

Para Lima (2020, p. 255), são múltiplas as missões da ANPD para cumprir as competências que lhe são atribuídas no artigo 55-J da LGPD[143]: “consultiva, de fiscalização, de

[143] “Art. 55-J. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2.º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei n.º 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir

controle, extrajudicial, administrativa, consultiva, promover a iniciativa de leis, de cooperação internacional com o objetivo de assegurar a proteção de dados pessoais".

Assim, a ANPD tem competência preventiva, regulatória, fiscalizadora, sancionatória, reparatória e educativa com base no tripé governo, mercado e sociedade, seguindo a lógica do compartilhamento de autoridade. A ANPD garantirá que as práticas mercadológicas sigam uma premissa preventiva na proteção de dados pessoais e uma premissa repressiva na punição de práticas danosas por uso indevido de dados pessoais. Desempenhará funções de fiscalização, de regulação e de sanção, sem excluir as boas práticas dos agentes de tratamento de dados. Além disso, a ANPD tem função mediadora entre interesses da pessoa humana e do mercado (LUCCA; LIMA, 2020, p. 376-377).

A cooperação, tanto internacional[144], como nacional, é um elemento de destaque na atuação da ANPD "a fim de facilitar as competências regulatória, fiscalizatória e punitiva"[145] (VERBICARO; VIEIRA, 2021a, p. 217). Mas, de acordo com o artigo 55-K da Lei n.º 13.853/2019, a ANPD é o órgão central e exclusivo para imposição de sanções, prevalecendo a

que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei n.º 10.741, de 1.º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. § 1.º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. § 2.º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório. § 3.º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei. § 4.º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD. § 5.º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei. § 6.º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada".

[144] É importante destacar as diretrizes da OCDE sobre a autoridade de proteção de dados, particularmente a sua atuação transfronteiriça (*protection of privacy and transborder flows of personal data*), não se podendo impedir a circulação de dados, desde que haja o mesmo nível de proteção (adequação). A LGPD, em seus artigos 33 a 36, dispõe que cabe à ANPD a atuação na proteção da transferência internacional de dados por meio de regulação procedimental própria.

[145] Ver o artigo 55-J, IX e § 4.º, da Lei n.º 13.853/2019.

sua decisão no contexto de proteção de dados pessoais graças a sua competência de fiscalização e de controle, que se exerce nas seguintes ações:

> requisitar informações dos responsáveis pelo tratamento de dados, ao titular dos dados e a terceiros quando for o caso, além de realizar diligências, procedimentos de autoria e inspeções em entidades públicas e privadas que realizam atividades de tratamento de dados pessoais (LIMA, 2020, p. 259).

Frisa-se, ainda, a estimulação da adoção de padrões técnicos (artigo 55-J, X, da LGPD) em atenção aos princípios da transparência e ao direito-dever à informação do usuário. O sistema, ao utilizar interfaces mais amigáveis, deve assegurar um ambiente seguro na coleta, no tratamento e na transferência de dados pessoais. Padrões obscuros são fonte de vulnerabilidades, e a atuação de uma entidade autônoma e independente[146] para controle e fiscalização deverá garantir a redução das desigualdades, evitando não apenas o dano em si, mas o estado de danosidade do consumidor inserido no contexto estudado:

> A regulação com base em leis e códigos nem sempre será eficiente no mundo desmaterializado, despersonalizado e desterritorializado como o ciberespaço. Portanto, as alternativas tecnológicas com base nos códigos de programação (*softwares*) podem ser utilizadas para garantia de direitos fundamentais, tais como a privacidade e a proteção de dados pessoais (LIMA, 2020, p. 260).

A atuação da ANPD atingirá um número indeterminado de consumidores (o consumidor por equiparação – *bystander* – ou a coletividade). Quanto à reclamação individual dirigida à ANPD (artigo 55-J, V, da LGPD), pode-se citar o direito à desindexação. Na tutela coletiva, o objetivo é a participação social, por meio da educação e da informação. De fato, medidas de participação coletiva, como audiências públicas e outras, favorecem a participação social no debate político qualificado (VERBICARO; VIEIRA, 2021b), garantindo o equilíbrio dinâmico entre os envolvidos.

O CNPDP tem especial importância no desenvolvimento de políticas públicas, fornecendo subsídios à ANPD para elaborar a PNPDPP.

Ainda, de acordo com o artigo 41, parágrafo 3, da LGPD, a ANPD "poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive em hipóteses de dispensa da necessidade de sua indicação" (artigo 55-J, II, da LGPD), bem como complementar e atualizar a lei à luz do código de boas práticas.

Desde a Diretiva 95/46/EC (UNIÃO EUROPEIA, 1995), os códigos de boas práticas são considerados instrumentos da regulação uma vez que são regras específicas do setor, elaboradas pelos próprios *players*. No mesmo sentido, segundo o artigo 40 do Regulamento

[146] Doneda (2019, p. 315) afirma que a independência da autoridade deve ser uma atribuição fundamental em razão da tutela do cidadão e da estruturação do sistema normativo, o que compreende a regulação do fluxo de dados.

(UE) 2016/679 (UNIÃO EUROPEIA, 2016), empresas e associações civis, estimuladas pelo setor público, podem elaborar essas regras. No Brasil, segundo o artigo 50 da LGPD, os agentes de tratamento de dados podem elaborar os respectivos códigos de boas práticas, que podem ser reconhecidos e divulgados pela ANPD (LIMA, 2020, p. 270), sem que isso contrarie a norma em sentido amplo.

Diversamente do que se esperava, a ANPD está vinculada à Presidência da República. É composta pelo CNPDP, que tem 23 titulares, não remunerados, com mandato de dois anos, oriundos de diferentes setores: seis do Executivo Federal, um do Senado Federal, um da Câmara dos Deputados, um do Conselho Nacional de Justiça, um do Conselho Nacional do Ministério Público, um do Comitê Gestor da Internet no Brasil, quatro da sociedade civil, com atuação comprovada em proteção de dados pessoais, quatro de instituição científica, tecnológica e de inovação e quatro de entidade do setor empresarial ligado à área de tratamento de dados pessoais[147]. Trata-se, pois, de uma composição multissetorial, que "propicia um natural sistema de freios e contrapesos interna corporis, colaborando para autonomia técnica da ANPD, pois os representantes do setor privado serão constantemente fiscalizados pelos representantes do setor público e vice-versa" (LUCCA; LIMA, 2020, p. 383).

A ANPD deve ser composta por um corpo técnico especializado – jurídico e técnico de tratamento de dados pessoais – para uma atuação de cunho repressivo, como também educativo, de orientação, adotando parâmetros que garantam a adaptação da lei a novas e constantes circunstâncias (DONEDA, 2019, p. 316).

Vale ressaltar a necessidade de atuação conjunta e convergente com a Senacon, que desempenha um papel essencial na fiscalização e na prevenção do uso indevido de dados pessoais do consumidor. Cabe lembrar que a ANPD ainda se encontra em fase de construção.

Em 2018, a Senacon requereu informação ao Facebook em razão do uso indevido de dados dos usuários pela Cambridge Analytica, solicitando:

> Qual é o alcance do suposto compartilhamento irregular? Ou seja, qual é o número de usuários brasileiros afetados por ele? Qual era a finalidade da captura dos dados dos consumidores? Detalhe e esclareça. Segundo as notícias, os usuários teriam concordado em fazer um "teste" online e teriam consentido em compartilhar seus dados "para fins acadêmicos". Essa informação procede? Se não, como os dados dos usuários brasileiros foram compartilhados com a Cambridge Analytica? Informe. Informe se, além da Cambridge Analytica, os dados compartilhados foram também disponibilizados a outras empresas sem que o usuário brasileiro tenha dado consentimento específico para tal. O Facebook tem parceria, contrato ou qualquer vínculo com empresa que promova o marketing político partidário no Brasil? Em caso afirmativo, explique. Depois da assunção do compartilhamento irregular, por parte da empresa, o que o Facebook fez ou está fazendo para contornar o problema?

[147] Ver o artigo 58-A da Lei n.º 13.853/2019.

> Especifique as ações tomadas de forma minuciosa. Como o Facebook age para proteger os dados de seus usuários e de que instrumentos dispõe para que essa proteção seja efetiva? (BRASIL, 2019b, p. 2).

A empresa Facebook manifestou-se, alegando que suas regras e atividades estavam em conformidade com as leis brasileiras, que houve consentimento ativo, que proíbe a venda e o compartilhamento de dados e, especialmente no caso investigado, que o compartilhamento foi feito sem autorização do Facebook[148]. Diante da manifestação da empresa, foi instaurado um processo administrativo por possível violação dos artigos 4.º, *caput*, incisos I, III e IV, 6.º,

[148] "Facebook Brasil apresentou as seguintes alegações preliminares: 01) que é uma empresa brasileira, constituída e existente em conformidade com as leis do Brasil e que tem por objeto social a prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade, suporte de venda etc.; 02) que o site http://facebook.com ('Site Facebook') é administrado e operado pelas entidades Facebook Inc. (norte-americana) e Facebook Ireland Limited, sendo a última a entidade responsável pela prestação dos serviços Facebook em todos os países, inclusive o Brasil; 03) que teria contatado Facebook Ireland e obtido as informações investigadas nos presentes autos; 04) que, segundo noticiado pela Facebook Ireland, a Cambridge Analytica, teria usado indevidamente dados de usuários do Facebook, os quais lhe foram repassados por um desenvolvedor de aplicativos, Dr. Aleksandr Kogan, em violação à Política de Uso da Plataforma Facebook, por meio de um aplicativo chamado thisisyourdigitallife; 05) que o aplicativo do Dr. Kogan fez uso do Facebook Login, um recurso da plataforma que permite que terceiros desenvolvedores de aplicativos solicitem o consentimento de usuários do Facebook para que seus aplicativos acessem categorias específicas suas; 06) que, na época, o Facebook Login admitia que os desenvolvedores solicitassem consentimento dos usuários para acessar categorias específicas de dados compartilhados com esses usuários por seus amigos no Facebook; 07) que entretanto, o Facebook Login sempre proibiu que desenvolvedores vendessem, licenciassem ou compartilhassem dados de usuários acessados do Facebook com qualquer rede de publicidade, corretora de dados ou outro serviço relacionado à publicidade ou monetização; 08) que, no caso dos autos, o Dr. Kogan transferira, em desobediência às políticas de uso da plataforma, alguns dados de usuários do Facebook que ele obteve por intermédio do aplicativo para a empresa responsável Cambridge Analytica (controlada por SCL Elections Limited), sem que houvesse autorização do Facebook e em violação à Política da Plataforma; 09) que os dados solicitados pelo Aplicativo e que foram consentidos pelos usuários eram: a) dados do perfil público, incluindo nome e gênero; b) data de nascimento; c) 'cidade atual' indicada na seção sobre perfil do usuário, se informada; d) páginas que o usuário curtiu; e) lista de amigos e, quanto a estes, as mesmas informações acima (dependendo e conforme as configurações de privacidade de cada amigo), ressalvando, ainda, que os dados repassados não envolviam senhas ou transações financeiras; 10) que o caso não se constitui em incidente de invasão de sistemas ou quebra de sigilo de dados (data breach); 11) que, ao ter ciência dos fatos, a Representada adotou Nota Técnica 32 (10626247) SEI 08012.000723/2018-19 / pg. 2 providências como: a) encerramento dos direitos de acesso do Aplicativo do Dr. Aleksandr à Plataforma Facebook em 17 de dezembro de 2015, (tendo tomado conhecimento do caso em 12 de dezembro de 2015); b) instituição de obrigação de que fossem apagados todos os dados obtidos pelo Aplicativo; c) banimento do acesso à plataforma à empresa Cambridge Analytica e ao do Dr. Kogan; 12) que foram ainda introduzidas mudanças na Plataforma Facebook, a partir de 30 de abril de 2014, com o objetivo de restringir os dados que aplicativos como o Dr. Aleksandr eram capazes de acessar; 13) que, quanto à extensão do número de usuários atingidos no Brasil, o Facebook entendeu que 84 (oitenta e quatro) pessoas no Brasil instalaram o Aplicativo, o que representava 0,03% do total de instalações do Aplicativo no mundo e que, no máximo 443.033 (quatrocentos e quarenta e três mil e trinta e três) pessoas adicionais no Brasil foram potencialmente afetadas. O número total máximo de 443.117 (quatrocentos e quarenta e três mil, cento e dezessete) pessoas foram potencialmente afetadas no Brasil, o que representa 0,51% do número global de pessoas potencialmente afetadas; 14) que teria assumido os seguintes compromissos adicionais para tratar da privacidade de dados em sua plataforma: a) revisão e auditoria da plataforma para fins de verificação de acessos a grandes quantidades de dados de usuários e identificação de mau uso de informação pessoal identificável; b) comunicação dos usuários sobre o mau uso de dados fornecidos à plataforma; c) interrupção do acesso a um aplicativo que esteja sem uso por mais de três meses; d) maior escrutínio na disponibilização de dados por meio da plataforma Facebook Login; e) maior estímulo à participação do usuário no controle dos dados disponibilizados à plataforma; f) instituição de um programa de recompensas para quem identificar vulnerabilidades" (BRASIL, 2019b, p. 2-3).

incisos II, III, IV e VI, 18, 31, 37 e 43 da Lei n.º 8.078/1990, bem como do direito à privacidade e à intimidade, nos termos da CF.

Em decisão, foi considerado que a) o modelo de negócio implicava um padrão de compartilhamento automático de dados pessoais dos amigos do usuário e b) houve falha no direito-dever à informação, o que configura prática abusiva e compartilhamento indevido de dados pessoais, com base nos artigos 4.º, *caput*, I, III e IV, 6.º, II, III, IV e VI, 18, 31, 37, *caput*, e 39, todos do CDC, e nas disposições do Marco Civil da Internet, notadamente, os artigos 2.º, II e III, e 7.º, VI, VII, VIII, IX e XIII. Assim, diante da exposição da coletividade de consumidores à lesividade, o Facebook foi multado em R$ 6.600.000,00 (seis milhões e seiscentos mil reais), em depósito no Fundo de Defesa de Direitos Difusos (BRASIL, 2019b, p. 1).

Ademais, em janeiro de 2020, após uma publicação pela Reuters sobre uso indevido de dados para fins publicitários por meio de assédio de consumo direcionado, a Senacon requereu uma série de explicações da Rappi sobre o tratamento de dados pessoais dos consumidores em consonância com o CDC e o Marco Civil da Internet:

> a) Essa entidade obtém o consentimento do consumidor para que possa fazer operações de tratamento de seus dados? Em caso positivo, para quais fins esse tratamento é realizado (publicidade direcionada de produtos e/ou serviços ou outros)? Em caso positivo, explicitar de que forma esse consentimento é obtido, contextualizando a obtenção desse consentimento no procedimento de adesão do consumidor ao ecossistema do aplicativo, com exposição das janelas e caixas de diálogo em que são inseridos os termos desse consentimento.
> Ainda, deverá a empresa demonstrar como esse consentimento se encontra em conformidade no que se refere ao Marco Civil da Internet, especialmente quanto aos arts. 7.º, incs. VII, VIII, IX e XI, e quanto ao modo pelo qual o consumidor é informado a respeito disso.
> b) Ainda, em sendo o caso, quais operações de tratamento de dados essa entidade executa? Há fornecimento de dados de consumidores para outras entidades? Para quais finalidades e para quem essa entidade executa operações de tratamento de dados de consumidores? Por fim, demonstrar como se dá o atendimento do legítimo interesse nas operações de tratamento (RIBAS, 2020, p. 1).

A Senacon emitiu a Nota Técnica 4/2019 sobre a competência da ANPD, indicando eventuais divergências na atividade entre os órgãos e ressaltando a necessidade de atuação conjunta: a "competência preponderante da ANPD pode colocar em risco o andamento e *enforcement* dos processos administrativos em andamento" (BRASIL, 2019a, p. 2).

Em março de 2021, a ANPD e a Senacon assinaram um acordo de cooperação técnica com os seguintes objetivos: a) apoio institucional e intercâmbio de informações relativos aos campos de atuação; b) compartilhamento de informações agregadas e dados estatísticos quanto às reclamações de consumidores, especialmente na base de dados do Sistema Nacional de Informações de Defesa do Consumidor (Sindec); c) uniformização de entendimentos e atuação

coordenada entre os órgãos, especialmente nos incidentes de segurança, a fim de garantir e de proteger os direitos dos consumidores; d) desenvolvimento de indicadores conjuntos relacionados à proteção de dados pessoais dos consumidores; e) elaboração conjunta de notas técnicas, estudos, análises, projetos de pesquisa, entre outros; f) organização e promoção de ações conjuntas, cursos, seminários e materiais informativos; g) cooperação nas ações de fiscalização.

Vale ressaltar a atuação conjunta da ANPD, da Senacon, do Conselho Administrativo de Defesa Econômica (Cade) e do Ministério Público Federal contra possíveis violações dos direitos do consumidor, especialmente a assimetria informacional, que desrespeita o artigo 11 do Marco Civil da Internet, eventual abuso pela ausência de mecanismo *opt-out* e de liberdade de escolha. Além disso, a ausência de transparência nos termos de privacidade configura publicidade enganosa e abusiva (artigos 31, 37, 38 e 39 do CDC), uma vez que a oferta não precifica o uso do serviço pelo consumidor (BRASIL, 2021). Em uma recomendação sobre a nova política de privacidade da empresa WhatsApp, os órgãos estipularam[149]:

> (A) ao WHATSAPP INC:
> (I) proceder ao adiamento da vigência de sua Política de Privacidade enquanto não adotadas as recomendações sugeridas após as análises dos órgãos reguladores;
> (II) abster-se de restringir o acesso dos usuários às funcionalidades do aplicativo, caso estes não adiram à nova política de privacidade, assegurando-lhes a manutenção do atual modelo de uso e, em especial, a manutenção da conta e o vínculo com a plataforma, bem como o acesso aos conteúdos de mensagens e arquivos, pois configuraria conduta irreversível com potencial altamente danoso, inclusive aos direitos dos consumidores, antes da devida análise pelos órgãos reguladores competentes;
> (III) adotar as providências orientadas às práticas de tratamento de dados pessoais e de transparência, nos termos da LGPD, conforme Relatório n.º 9/2021/CGF/ANPD e Nota Técnica n.º 02/2021/CGTP/ANPD;
> (B) Ao FACEBOOK MIAMI INC., ao FACEBOOK GLOBAL HOLDINGS III, LLC, ao FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA., sociedade empresária limitada que possui como únicas sócias as duas primeiras pessoas jurídicas citadas, e a quaisquer outras empresas do grupo FACEBOOK:
> (I) abster-se de realizar qualquer tipo de tratamento ou compartilhar dados recebidos a partir do recolhimento realizado pelo WhatsApp Inc. com base nas alterações da Política de Privacidade do aplicativo previstas para entrar em vigor no dia 15 de maio de 2021, enquanto não houver o posicionamento dos órgãos reguladores (BRASIL, 2021, p. 8).

[149] Na atualização da sua política de privacidade, o WhatsApp ampliou o compartilhamento de dados pessoais com o Facebook, bem como impossibilitou a negativa de consentimento nessa nova política por meio de sua aplicação bifásica, diversamente da política adotada na União Europeia. A ANPD requereu uma série de esclarecimentos: tipos de dados compartilhados; informações adicionais sobre os agentes de tratamento; fonte dos dados pessoais; forma de armazenamento e compartilhamento; finalidade do compartilhamento e tratamento; base legal e justificativa de aplicação; forma de obtenção do consentimento, se aplicável; forma e consequência da recusa do consentimento; forma de concessão dos direitos determinados no artigo 18 da LGPD; mecanismos de segurança. Isso ensejou o Processo Administrativo n.º 00261.00012/2021-04.

Em manifestação, a empresa WhatsApp comprometeu-se a não restringir o acesso ao serviço daqueles que não consentirem na nova política, adotar uma adaptação gradual nos 90 dias (a contar de 14 de maio de 2021), além de discutir com as autoridades competentes sobre possíveis preocupações e soluções quanto ao tratamento de dados[150].

A ANPD tem, portanto, um poder-dever normativo, com competência para editar regulamentos e procedimentos sobre proteção de dados e para interpretar dispositivos estabelecidos na LGPD, além do poder-dever disciplinar ou sancionatório na função fiscalizatória, para exercer uma tutela preventiva e punitiva (LUCCA; LIMA, 2020, p. 393). A sua autonomia decisória e técnica é essencial na busca de uma atuação mediadora tendo em vista o equilíbrio mercadológico e o desenvolvimento de uma economia de dados pessoais harmoniosa entre os agentes envolvidos.

5.2.2 Política Nacional de Proteção de Dados Pessoais e da Privacidade

Em atenção aos artigos 55-J, III, e 58-B, I e II, da LGPD, compete à ANPD elaborar diretrizes para a PNPDPP. De acordo com o artigo 58-B, a CNPDP tem as seguintes atribuições:

> I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
> II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> III - sugerir ações a serem realizadas pela ANPD;
> IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade;
> V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Atualmente, o CNPDP está em processo de escolha de seus conselheiros por meio de uma lista tríplice a ser encaminhada ao presidente da República[151]. Por conseguinte, a PNPDPP, até o presente momento, ainda não saiu da intenção.

O artigo 4.º do CDC define a PNRC. É importante frisar o seu caráter instrumental no compartilhamento da autoridade. Sua atuação extrapola a estipulação de normas administrativas, buscando o exercício harmonioso entre os agentes inseridos na relação, tendo o Estado como mediador dos interesses conflitantes. Explica Verbicaro (2017, p. 541):

> A partir dos artigos 4.º e 5.º da Lei n.º 8.078/1990, o Direito do Consumidor ganhou uma roupagem diferente e se tornou um Direito do Consumo, porque busca um equilíbrio de forças entre o Estado, o consumidor e o fornecedor, estabelecendo metas,

---

150 Ver https://exame.com/tecnologia/whatsapp-vai-permitir-acesso-a-quem-nao-concordou-com-novos-termos-de-uso/.

151 Ver https://www.gov.br/anpd/pt-br/composicao-1/conselho-nacional-de-protecao-de-dados-pessoais-e-privacidade-cnpd.

> princípios, prioridades e ações concretas. Esse ordenamento possibilita: minimizar a falta de interesse governamental em uma tutela efetiva do consumidor; combater a falta de receptividade do segmento empresarial à mudança de comportamento ético, através do aprimoramento tecnológico da qualidade e da segurança dos produtos e serviços colocados no mercado – que, naturalmente, impactam a margem de lucro dos fornecedores – bem como estimular um maior nível de interesse gregário do consumidor em se articular como categoria e não mais apenas sob a ótica individual.

A PNRC, portanto, tem caráter programático e dirigente: ao estabelecer a proteção de grupos desiguais, reflete o ideal de solidariedade, reforça novos espaços de participação cívica, defende a boa-fé objetiva, a harmonia e a educação na relação de consumo.

O objetivo é garantir o equilíbrio na relação tão desigual. O Estado atuará como mediador entre os atores e como fiscalizador, inclusive de empresas públicas consideradas fornecedoras de produtos e serviços. Deverá ainda implementar instrumentos que possibilitem a redução do exercício da tutela consumerista, especialmente nos termos do artigo 5.º do CDC.

Embora a PNPDPP ainda não exista, constata-se que a essência legislativa relacionada ao mercado informacional visa a harmonia entre as partes por meio da adoção de práticas preventivas e de segurança, considerando ainda a proporcionalidade entre o tratamento de dados e a proteção do consumidor. De igual modo, na PNRC, o Estado será o mediador entre as ações do consumidor, considerado vulnerável na relação, e os agentes de tratamento de dados, considerados, por equiparação, fornecedores.

De um lado, a PNPDPP deve defender a prevenção do estado de danosidade e a repressão dos danos, a regulação e a aprovação de códigos de boas práticas que visam garantir condutas mercadológicas éticas. De outro lado, devem ser implementadas políticas educativas e de orientação com o objetivo de empoderar o consumidor. Uma coordenação de órgãos de proteção dos dados pessoais, inseridos em uma Política Nacional, deve possibilitar o exercício da cidadania instrumental.

O Instituto Brasileiro de Defesa do Consumidor (Idec) analisou a atuação das ANPD latino-americanas – da Argentina, do Uruguai e da Colômbia – para avaliar a sua efetividade. Foi considerado como padrão de estudo o dever educativo (SIMÃO; OMS; TORRES, 2019).

Tabela 5 – ANPD na Argentina.

Argentina		
Criação	**Órgão**	**Dever educativo**
Criada em 2000, pela Lei n.º 25.326/2000, tendo sido regulamentada pelo Decreto n.º 1558/2001. Em 2017, sua estrutura foi modificada, passando a integrar a Agencia de Acceso a la Información	Dirección Nacional de Protección de Datos Personales	Passou a exercer o dever educativo a partir da reforma legal, por meio da difusão de capacitações. Apesar dessa atuação, reconhece-se sua pouca efetividade. Há necessidade de maior consciência por parte da população. Baixo número de denúncias.

Pública (administração indireta do Estado argentino).		

Fonte: SIMÃO, OMS, TORRES, 2019.

Tabela 6 – ANPD na Colômbia.

Colômbia		
Criação	**Órgão**	**Dever educativo**
A lei de proteção de dados pessoais colombiana (Lei n.º 1.581/2012) atribuiu as funções da autoridade nacional à Superintendência de Indústria e Comércio (SIC). A Superintendência criou uma pasta específica nomeada "Delegatura de proteção de dados pessoais", que, em 2015, passou a fazer parte da administração descentralizada, ganhando personalidade jurídica própria.	Delegatura de proteção de dados pessoais Superintendência de Indústria e Comércio (SIC)	Produção de cartilhas e materiais para explicar à população como funcionam seus direitos e os mecanismos disponíveis para seu exercício. Aos poucos, a população obtém conhecimento sobre a necessidade de proteção de seus dados. A falta de recursos é o maior obstáculo para a difusão de conhecimentos.

Fonte: SIMÃO, OMS, TORRES, 2019.

Tabela 7 – ANPD no Uruguai.

Uruguai		
Criação	**Órgão**	**Dever educativo**
A Unidad Reguladora y de Control de Datos Personales foi criada pela Lei de Proteção de Dados Pessoais e Ação de Habeas Data (Lei n.º 18.331/2008). A Unidad é um órgão desconcentrado da Agência para o Desenvolvimento de Gestão Eletrônica, da Sociedade da Informação e do Conhecimento (Agesic), vinculada à Presidência da República.	Unidad Reguladora y de Control de Datos Personales	São elaboradas campanhas e materiais didáticos pela autoridade. Constata-se que cerca de 51% da população conhece a lei e seus direitos básicos. Apesar desse trabalho, "a representante da sociedade civil avalia que falta capacidade e estratégia para chegar aos atores principais, como a consolidação de uma rede de inspeção e trabalho preventivo" (SIMÃO; OMS; TORRES, 2019, p. 34).

Fonte: SIMÃO, OMS, TORRES, 2019.

Observa-se que a falta de políticas educacionais impossibilita o exercício ativo do consumidor contra práticas consideradas indevidas no tratamento de dados pessoais. A PNRC destaca a necessidade de formulação de uma política destinada a promover a educação para o consumo, devendo a PNPDP também seguir a mesma linha.

Por outro lado, as associações de proteção dos dados pessoais têm essencial importância por representarem "uma força contramajoritária em relação ao poder econômico dos fornecedores", incentivando a conexão entre os cidadãos e a real consecução das políticas públicas (VERBICARO, 2017, p. 546). No Brasil, é possível observar uma atuação positiva das

associações de proteção dos dados pessoais, destacando-se InternetLab, CodingRights, Íris, Lapin, Data Privacy Brasil, Idec, Brasilcon, entre outras.

5.3 Controle dos *gatekeepers:* aspectos preventivos e estruturais

A LGPD, além do combate a práticas danosas por meio da imputação da responsabilidade, estruturou práticas preventivas. Assim, agentes de tratamento de dados devem adotar políticas de segurança, como se infere dos artigos 46 e 6.º, VIII.

Como se viu no capítulo 4, a legislação visa impedir condutas que exporiam o usuário consumidor a um estado de danosidade. Daí a necessidade de adoção de mecanismos operacionais e preventivos. A LGPD apresenta uma dubiedade na configuração da obrigação legal dos agentes de tratamento de dados de impor o princípio da responsabilidade e da prestação de contas (*accountability*) no sentido de se adotarem medidas eficazes no tratamento de dados com comprovado atendimento aos preceitos legais.

No mesmo sentido, Mendes e Fonseca (2020, p. 523) ressaltam que a finalidade regulatória está pautada pela *accountability* na proteção de dados, com a implementação de estratégias de mitigação de riscos e de transparência. A prevenção e a prestação de contas não estão apenas na responsabilização em si, mas desde a concepção da atividade do fornecedor, com a aplicação de regras de *compliance*, governança e *privacy by design*, como previsto nos artigos 50 e 51 da LGPD:

> Por força do que explicita o § 2.º, deve-se assim proceder desde a concepção do produto ou serviço, o que indica um imperativo amplo de controle e proteção que não se limita apenas ao tratamento de dados, per se, mas a todas as etapas relacionadas a atividade que, potencialmente, contemplem o tratamento (MARTINS; FALEIROS JÚNIOR, 2020, p. 351).

O objetivo é redefinir o limiar de responsabilização para além da ocorrência do dano, buscando-se práticas de tratamento de dados coesas, em observância ao efetivo consentimento ativo, quando for a base legal autorizadora. Evita-se, assim, a configuração do estado de danosidade do consumidor. É o que exige a governança "a partir de emanações concernentes à boa-fé objetiva, à inserção ética nas relações negociais, à prevenção e à efetivação dos direitos fundamentais à privacidade e à proteção de dados pessoais" (MARTINS; FALEIROS JÚNIOR, 2020, p. 357).

Em outro sentido, é a expressão do compartilhamento da autoridade política, uma complementação da regulação estatal, por meio de incentivos, seja pela prática de empoderamento do consumidor pela cidadania instrumental, seja pelo estabelecimento de

condutas éticas mercadológicas tendo em vista a fidelização da marca, o que consequentemente exige um controle maior contra violações de direitos dos titulares.

5.3.1 Governança, boas práticas e *compliance*

A LGPD, em seus artigos 46 a 51, trata da adoção dos princípios da segurança e da prevenção, especialmente com a adoção de boas práticas no tratamento de dados pessoais. No que diz respeito à governança dos dados, são necessárias "medidas adequadas para fornecer ao titular as informações legais e qualquer comunicação a respeito do tratamento a ser empreendido, de forma concisa, transparente, inteligível e de fácil acesso" (SIMÃO FILHO, 2020, p. 328). De acordo com o artigo 49 da LGPD, os sistemas de tratamento de dados pessoais devem ser estruturados para cumprir os requisitos de segurança, os padrões de boas práticas e de governança e os princípios gerais previstos na LGPD (MARTINS; FALEIROS JUNIOR, 2019, p. 357).

Para Arnaud (2014, p. 273-275), o conceito de governança diz respeito à construção de uma política capaz de atuar de forma cooperativa entre atores, grupos sociais e instituições, à elaboração de um programa capaz de articular lógicas divergentes na tentativa de alcançar o consenso. A governança envolve uma metodologia positiva, a individualização dos princípios e mecanismos que compõem o sistema, a harmonização de condutas, a otimização de regras (SIMÃO FILHO, 2020, p. 329) com a finalidade de atingir o mercado consumidor e investidor pela adoção de padrões que consideram aspectos sociais.

O programa de governança de dados possibilita o contínuo monitoramento e a constante atualização por meio do estabelecimento de regras para aplicação de mecanismos internos e externos. Nesse sentido, cabe destacar que o artigo 50 da LGPD prevê a formulação, pelos controladores, operadores e associações, de regras de boas práticas e de governança que estabeleçam as condições organizacionais, o regime de funcionamento, as normas de segurança, os padrões técnicos, as obrigações específicas, as ações educativas, os mecanismos de mitigação de riscos. Esses princípios de segurança e de prevenção (SIMÃO FILHO, 2020, p. 342-343) devem ser reconhecidos pela ANPD.

O cumprimento dos padrões de segurança, das boas práticas, da governança e dos princípios previstos na legislação exige a adoção de *compliance* no tratamento de dados:

> Nesse contexto, quando se fala em compliance digital a partir de mecanismos de segurança, é possível enumerar, dentre vários instrumentos, a autenticação multinível, as ferramentas criptográficas, o controle de acesso a banco de dados, a prevenção à exposição a sofware de natureza maliciosa e aos ataques de denial-of-service, a detecção de vulnerabilidades e intrusões, o uso de firewalls e sistemas de prevenção, os controles de buffer, os sistemas operacionais e a segurança de sistemas de

> armazenamento em nuvem como singelos exemplos de gargalos dos quais não se prescinde na edição de uma lei que pretenda tutelar contingências de envergadura tão complexa (MARTINS; FALEIROS JÚNIOR, 2020, p. 358).

Segundo Frazão, Oliva e Abilio (2019, p. 686), as vantagens tradicionalmente atribuídas aos programas de *compliance* são:

> (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas.

Para as autoras, a essas vantagens, soma-se, na tutela de dados, a vantagem adicional de adaptar e operacionalizar diversos comandos gerais e conceitos abertos da LGPD.

Frazão, Oliva e Abilio (2019, p. 687-693) enumeram 10 requisitos-padrão para a adoção de regras de *compliance*: avaliação contínua de riscos e atualização de programa; elaboração de Códigos de Ética e de Conduta; organização estrutural compatível com o risco da atividade; comprometimento da administração; independência e autonomia do setor de *compliance*; treinamentos periódicos; criação de uma cultura corporativa de respeitos à ética e às leis; monitoramento constante de controle e processos; canais seguros de comunicação de infrações e mecanismos de proteção dos informantes; detecção, apuração e punição de condutas contrárias ao programa de *compliance*.

Em harmonia com os requisitos citados, os artigos 37, 38, 44, parágrafo único, 46 e 50, parágrafos 1.º e 2.º[152], da LGPD enunciam diretrizes para o programa de *compliance* esperado,

---

[152] "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1.º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. § 2.º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6.º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II - demonstrar a efetividade de seu programa de governança em privacidade

estabelecem parâmetros a serem incorporados e estruturados pelos agentes de tratamento de dados de forma eficaz de acordo com os ditames legais. Ainda, o atendimento dos critérios aduzidos no artigo 50 da LGPD pode ser considerado a excludente de responsabilidade prevista no artigo 43, II, dessa lei em conformidade com os padrões exigidos na legislação.

É importante mapear todo o ciclo de tratamento de dados a fim de observar se os direitos dos titulares estão sendo preservados em todo o processo. Nesse sentido, o relatório de impacto é valioso para a implementação da ferramenta de *compliance* por apresentar tais informações, em atenção ao artigo 38 da LGPD. Frazão, Oliva e Abilio (2019, p. 700) destacam a necessária avaliação de todo o ciclo de tratamento de dados, considerando (a) o momento de utilização dos dados pessoais, b) os tipos de dados, c) como e quem os coletou, d) como sua utilização liga-se à finalidade da atividade, e) o controle organizacional para a definição de condutas e estipulação de sistemas que possibilitam o exercício de direitos dos titulares.

A análise do quantitativo de dados, da finalidade e da necessidade do tratamento também são instrumentos para garantir o cumprimento das regras que envolvem o tratamento (ir)regular, como previsto no artigo 44 da LGPD, em atenção, inclusive, às diretrizes de segurança. Nesse último aspecto, frisa-se que a identificação dos riscos no tratamento são a base para a formulação de regras de boas práticas e a formulação do programa de governança em privacidade.

As medidas organizacionais e estruturais impostas pelas regras de *compliance* resultam da adoção de uma metodologia centrada na privacidade do usuário desde a concepção – ***privacy by design*** – e possibilitam o exercício da base autorizativa de forma legítima pela correta identificação de riscos e pela implementação de procedimentos adequados e proporcionais:

> Por exemplo, no caso de tratamento com base no consentimento do titular, o código [de conduta] deve guiar os funcionários, determinando a obtenção de consentimento nos moldes dos arts. 8.º e 9.º, bem como assegurando-se que o tratamento se limitará à finalidade para a qual se destina. Os documentos devem estabelecer mecanismos de alerta para hipóteses mais sensíveis de tratamento, ou seja, aquelas em que há risco para o titular, permitindo aos funcionários identificar quais são essas hipóteses, bem como demonstrando cuidado intensificado nesses casos (FRAZÃO; OLIVA; ABILIO, 2019, p. 703).

Os mecanismos de *compliance,* portanto, concretizados na governança e nas condutas baseadas em boas práticas, afastam a responsabilidade do agente de tratamento, seja pela demonstração da excludente de responsabilidade (art. 43, II, da LGPD), seja pela demonstração do cumprimento de deveres, considerando inclusive a possibilidade de inversão do ônus da

---

quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei".

prova (FRAZÃO; OLIVA; ABILIO, 2019, p. 712). A adoção desses mecanismos também possibilitam um ganho reputacional e a construção de uma relação de confiança, por ensejarem a prestação de contas – *accountability* – e a, consequente, redução das vulnerabilidades do consumidor.

5.3.2 *Design* e *privacy by design*: a proteção da privacidade do usuário/consumidor como elemento central da construção de estratégias tecnológicas

Em 1998, na revista *Bloomberg Businessweek*, Steven Jobs afirmou: "Muitas vezes, as pessoas não sabem o que elas querem até você lhes mostrar". Com base na análise das diretrizes que devem ser seguidas na criação de redes, é arriscado confirmar o que disse Jobs. Na verdade, o desenvolvimento de um produto e/ou serviço exige critérios formais, cognitivos e relacionais.

É imperioso destacar o conceito de usabilidade na *web design* na concretização do direito-dever à informação do usuário. De acordo com Lowdermilk (2013, p. 26), usabilidade é a prestação de melhores serviços por meio da construção de produtos centrados no usuário.

O desenvolvimento de um produto ou serviço pautado por padrões obscuros[153] diminui a interatividade e a consequente confiança. Krug (2014, p. 13) afirma que "o fato de as pessoas responsáveis pela criação do site não terem se importado em deixar tudo óbvio – e fácil – pode diminuir nossa confiança e em quem está por trás dele".

Segundo Lowdermilk (2013, p. 26), o *design* centrado no usuário (DCU) é fruto da interação homem-computador. Trata-se de uma "metodologia de design de software para desenvolvedores e designers. Essencialmente, ajuda a criar aplicativos que atendam às necessidades dos usuários", mantendo uma boa usabilidade. Tem por objetivo economizar tempo, evitar equívocos e erros por entender e atender as expectativas dos usuários.

Os princípios do DCU são diretrizes baseadas na cognição e no comportamento humano em sua interação com o mundo: princípio da proximidade, princípio da visibilidade, princípio da proeminência visual, *feedback* visual, modelos mentais e metáforas, consistência e confirmação.

Como se viu, há concretas vulnerabilidades na relação de dados de consumo, e o *design* tem um papel primordial na desconstrução de assimetrias, especialmente no estabelecimento da

[153] Padrões obscuros (*dark patterns*) são "recursos de *design* de interface criados para induzir os usuários a fazer coisas que eles podem não querer, mas que beneficiam os negócios em questão" (HOW..., 2018, tradução nossa).

informação. Mas quais a diretrizes capazes de possibilitar o exercício do direito-dever informacional?

O princípio da proximidade está relacionado à organização e ao agrupamento de itens que simplifiquem a função e melhorem a experiência do usuário. Lowdermilk (2013, p. 98) frisa que "percebemos relacionamentos entre objetos que estão mais próximos. Inversamente, objetos que estão mais distantes, aparentemente, teriam menos relação".

O princípio da visibilidade harmoniza-se com o anterior ao estabelecer indicadores visuais para auxiliar a compreensão do *status* do aplicativo (LOWDERMILK, 2013, p. 113), em atenção à possibilidade do conhecimento da interação (*feedback* visual) e à utilização de objetos de fácil compreensão com cores fortes, fontes maiores e mais proeminentes (princípio da proeminência visual).

Modelos mentais e metáforas baseiam-se na realidade física dos usuários. De acordo com a consistência, os usuários aprendem e compreendem aquilo que já é conhecido, que funciona conforme o esperado (simplicidade). A confirmação é um modo de evitar ações indesejadas ao ser solicitada uma verificação (LOWDERMILK, 2013, p. 114).

Krug (2014, p. 34-45) destaca alguns pontos a serem observados na construção do *webdesign*, evidenciando projetos de painéis, hierarquia visual, divisão em áreas claras, minimização de confusão visual (complexidade e distrações), formatação de conteúdo, orientação breve, oportuna e inevitável.

A agradabilidade, a aprendibilidade e a inesquecibilidade também devem imperar na relação. Aplicativos agradáveis resultam "do casamento de uma ideia acerca de algo que as pessoas realmente adorariam ter como fazer, mas não imaginam que seja possível, com uma ideia fresca sobre como usar novas tecnologias para executar o que pretendem" (KRUG, 2014, p. 154). A inesquecibilidade é assim definida:

> um fator decisivo a indicar se as pessoas adotarão o aplicativo para o uso regular. Normalmente, quando você compra ou baixa um aplicativo, pretende gastar algum tempo dedicando-se a descobrir como usá-lo. Mas, se você tiver que gastar esse mesmo tempo toda próxima vez, a experiência se tornará insatisfatória. A menos que você seja muito impressionado pelo que ele faz, há uma boa chance de que o abandone (KRUG, 2014, p. 157).

Os recursos visuais visíveis e claros têm por finalidade explicitar os objetivos da navegação, capturar as características citadas e estabelecer um sentimento de confiança. Para Krug (2014, p. 166-167), são fatores que diminuem a confiabilidade: a) esconder informações comuns do fornecedor; b) reprimir por não seguir as regras impostas; c) solicitar informações pessoais desnecessárias; d) enganar; e) adotar padrões obscuros – *designs* confusos; f) agir com amadorismo – aparência desorganizada e não profissional.

Por outro lado, há fatores que aumentam a confiança na relação: a) entender seu público e tornar visível e fácil o acesso às informações; b) responder a perguntas (*feedback*); c) economizar etapas no meio do processo; d) empenhar-se e assegurar suporte técnico preciso, claro e direto; e) saber a quais perguntas provavelmente precisará de responder (*faq* atualizado e sincero; f) preparar páginas de impressão amigáveis; g) facilitar a recuperação de erros; h) pedir desculpas (KRUG, 2014, p. 168-169).

Para Kalbach (2017, p. 13), mapear experiências tem benefícios potenciais por ajudar na criação de empatia, fornecer uma imagem geral comum, reduzir a complexidade e encontrar oportunidades. Lowdermilk (2013) defende o estabelecimento da empatia por meio da criação de narrativas, *personas* e cenários na formulação do produto e serviço centrado nos usuários.

Uma narrativa é "uma história contínua de como o aplicativo molda as vidas dos usuários. Os manifestos são afirmações específicas e declarativas, enquanto narrativas podem ser enriquecidas com cenários detalhados sobre como o aplicativo será utilizado" (LOWDERMILK, 2013, p. 71). A *persona* é um personagem de ficção, uma personificação de usuários reais. Os cenários refletem situações reais para indicar os picos negativos a fim de melhorar a experiência do usuário.

Segundo Waldman (2018), não apenas as vulnerabilidades inerentes aos usuários, mas também o *design* obscuro da plataforma podem criar expectativas contrárias ao consumidor. A proteção da privacidade e a autodeterminação informacional no *design* são essenciais para a construção da confiança. A grande dificuldade na construção de *designs* de acordo com as políticas de privacidade é a falta de interação entre *designers* e os departamentos jurídicos. Daí a existência de plataformas que não cumprem a legislação de proteção de dados aplicada no território. Um exemplo de *design* que não protege a privacidade é o aplicativo Pokémon Go:

> [...] o popularíssimo aplicativo Pokémon Go também foi projetado sem ter a privacidade em mente. Em sua versão inicial, a plataforma acessou câmeras de smartphones dos jogadores, coletou dados de localização e, mais notavelmente, ganhou acesso total às contas Google dos jogadores, incluindo e-mail, calendários, fotos, documentos armazenados, e quaisquer outros dados associados ao login. O aplicativo era projetado desta forma. Para jogar Pokémon Go, os jogadores precisam de um conta. As contas podem ser criadas de duas maneiras: por meio de pokemon.com ou por meio do Google. Normalmente, quando um usuário do aplicativo faz login usando uma conta do Google, um pop-up explica quais dados o aplicativo será capaz de acessar, permitindo que o usuário decida prosseguir ou recusar com base nas práticas de uso de dados do aplicativo. Esse não era o caso do Pokémon Go. Em vez disso, os usuários faziam login usando o Google e imediatamente passavam para a interface do jogo. As permissões-padrão, que eram ocultas por design, davam ao Pokémon Go acesso à conta Google do jogador (WALDMAN, 2018, p. 676-677, tradução nossa)[154].

[154] No original: "More recently, the wildly popular Pokémon Go app was also designed without privacy in mind. In its initial release, the platform accessed players'smartphone cameras, collected location data, and, most notably, gained full access to players'Google accounts, including email, calendars, photos, stored documents,

O PbD – um princípio estabelecido na LGPD, especialmente nos seus artigos 46, parágrafo 2.º, e 6.º, VIII – engloba políticas de prevenção, de segurança da informação e de privacidade do usuário desde a concepção do produto ou serviço. Utiliza pricípios fundamentais do *design*, destacam-se a empatia, a simplicidade, a humildade e a informação, todos concorrendo para a construção de uma relação de confiança entre as partes, para a formulação de experiências consistentes por meio da criação de *personas*.

O modelo de construção do relacionamento base no *privacy by design* apresenta um estado-alvo fundamentado no compartilhamento de dados fluidos, conscientes e controlados, visando a instauração de confiança entre as partes por meio da maximização da experiência e da mimização do uso dos dados pessoais. É o reconhecimento da importância de incorporar os princípios da privacidade aos processos de concepção, de operação e de gestão de sistemas organizacionais com a finalidade de alcançar a proteção integral dos dados pessoais (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 5).

A metodologia PbD foi criada por Ann Cavoukian, especialista em privacidade de dados, e apresentada na 32.ª Conferência Internacional de Comissários para a Proteção de Dados e Privacidade, realizada em Jerusalém no período de 27 a 29 de outubro de 2010, ensejou a formulação da *Resolution on Privacy by Design*. Utilizando princípios do *design* na formulação de uma arquitetura de rede centrada no usuário, a metodologia impõe princípios-diretrizes, em atenção ao guia para PbD da Agência Espanhola de Proteção de Dados, publicado em outubro de 2019 (Tabela 8).

Tabela 8 – Diretrizes baseadas no Guia sobre PbD da Agência Espanhola de Proteção de Dados Pessoais.

Privacy by design		
Princípios-diretrizes	**Conceitos**	**Implementação**
Proativo, não reativo Preventivo, não reparador	Concebido e projetado desde o início, identificando possíveis riscos para os direitos e liberdades dos titulares dos dados e minimizando-os antes	• Assumir um compromisso claro com a organização a partir dos níveis mais altos da Administração. • Desenvolver uma cultura de compromisso e melhoria contínua por todos os trabalhadores. • Definir e atribuir responsabilidades concretas para que cada membro da organização esteja claramente ciente de suas tarefas no que diz respeito à privacidade.

and any other data associated with the login. The app was designed this way. In order to play Pokémon Go, players need an account. Accounts could be created in two ways: through pokemon.com or through Google. Normally, when an app user signs in using a Google account, a pop-up explains what data the app will be able to access, allowing the user to decide to go ahead or decline based on the app's data use practices. That was not the case with Pokémon Go. Rather, users signed in using Google and immediately proceeded to the game interface. The default permissions, which were hidden by design, gave Pokémon Go full access to the player's Google account".

	que possam causar danos reais	• Desenvolver métodos sistemáticos baseados em indicadores para a detecção precoce de processos e práticas deficientes na garantia da privacidade.
Privacidade como configuração padrão	A configuração padrão deve ser estabelecida por *design* que estabelece o nível máximo privacidade possível. […] Baseado na minimização de dados ao longo das etapas de processamento: compilação, uso, retenção e distribuição.	• Tornar os critérios de coleta de dados o mais restrito possível. • Limitar o uso de dados pessoais aos objetivos para os quais foram coletados e garantir que haja uma base legítima para o processamento. • Restringir o acesso aos dados pessoais às partes envolvidas no processamento de acordo com o princípio da "necessidade de saber" e de acordo com a função por trás da criação de perfis de acesso diferenciados. • Definir limites de tempo estritos para a retenção e estabelecer mecanismos operacionais que garantem o cumprimento de regras. • Criar barreiras tecnológicas e procedimentais para a ligação não autorizada de fontes independentes de dados.
Privacidade incorporada ao *design*	A privacidade deve ser parte integrante e inseparável dos sistemas, aplicativos, produtos e serviços, bem como das práticas e processos de negócios de uma organização.	• Considerar o *design* como um requisito essencial no ciclo de vida dos sistemas e serviços, bem como na concepção de processos organizacionais. • Realizar uma análise de risco dos direitos e liberdades das pessoas e, quando aplicável, realizar avaliações de impacto de proteção de dados, como parte integrante de qualquer nova iniciativa de processamento. • Documentar todas as decisões que são adotadas na organização a partir de uma perspectiva de PbD.
Funcionalidade total: soma positiva, não soma zero	Novas soluções para um funcionamento totalmente funcional	• Supor que interesses diferentes e legítimos podem coexistir: os da organização e os dos usuários a quem presta serviços, sendo necessário identificá-los, avaliá-los e equilibrá-los. • Estabelecer canais de comunicação para a colaboração e a consulta dos participantes a fim de compreender e reunir múltiplos interesses que, à primeira vista, podem ser divergentes. • Se as soluções propostas ameaçam a privacidade, buscar novas soluções e alternativas para alcançar a funcionalidade e os propósitos pretendidos, mas nunca perdendo de vista o fato de que os riscos à privacidade do usuário devem ser gerenciados de forma adequada.
Segurança de ponta a ponta: proteção total do ciclo de vida	A segurança da informação envolve confidencialidade, integridade, disponibilidade e resiliência dos sistemas que o armazenam. A privacidade também garante desvinculação, transparência e capacidade de intervenção e controle do titular dos dados no processamento (intervenção).	• Técnicas precoces de pseudoanonimização ou anonimato, como k-anonimato. • Classificação e organização de dados e operações de processamento com base em perfis de acesso. • Criptografia-padrão para que o estado "natural" dos dados, quando roubados, seja "ilegível". • Destruição segura e garantida da informação no final de seu ciclo de vida.
Visibilidade e transparência	Deve garantir a privacidade, verificando que o processamento está de acordo com as informações fornecidas.	• Elaborar as políticas de privacidade e proteção de dados que regem com os ditames legais. • Desenvolver e publicar informações concisas, claras e compreensíveis, cláusulas que são facilmente acessíveis e que permitem que os titulares dos dados entendam o âmbito do processamento dos seus dados, os riscos a que podem

		estar expostos e como podem exercer seus direitos em relação à proteção de dados. • Embora não seja obrigatório para todos os controladores, tornar pública, ou pelo menos facilmente acessível para os titulares dos dados, a lista de todos os processamentos realizados na organização. • Compartilhar a identidade e detalhes de contato do controlador de dados da organização. • Estabelecer mecanismos de comunicação acessíveis, simples e eficazes, compensações e reclamações para os proprietários dos dados.
Respeito pela privacidade do usuário	O objetivo final deve ser garantir os direitos e liberdades dos usuários cujos dados são processados. Portanto, qualquer medida adotada deve buscar garantir a sua privacidade. Isso envolve a concepção de processos "centrados no usuário", aplicações, produtos e serviços, antecipando as necessidades dos usuários.	• Implementar configurações de privacidade que são "robustas" por padrão e informar os usuários das consequências para a sua privacidade quando parâmetros forem modificados. • Disponibilizar informações completas e adequadas que conduzam a um consentimento informado, livre, específico e inequívoco que deve ser explícito em todos os casos que o exigem. • Fornecer aos titulares dos dados acesso aos seus dados e a informações detalhadas sobre as metas de processamento e comunicações realizadas. • Implementar mecanismos eficientes e eficazes que permitam que os titulares dos dados exerçam os seus direitos em matéria de proteção de dados.

Fonte: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, tradução nossa.

Tradicionalmente, projetos de sistema e arquitetura de rede concentram-se na análise de riscos e ameaças, tendo por base a confidencialidade, para evitarem o acesso não autorizado aos sistemas, a integridade, para protegerem contra alterações não autorizadas, e a disponibilidade, para garantir que os dados e sistemas estejam sempre disponíveis. No entanto, pelo aumento dos riscos e das ameaças, o Regulamento Geral sobre Proteção de Dados ampliou seu escopo de metas para incluir a *unlinkability*[155], a transparência e a *intervenability*[156] no quadro geral de proteção do processamento de dados (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 12-14).

A engenharia da privacidade é um processo sistemático orientado para o risco que visa traduzir em termos práticos e operacionais os princípios do PbD dentro do ciclo de vida dos sistemas de informação. Esse objetivo é alcançado por meio da delimitação das propriedades e funcionalidades da privacidade que devem ser observadas na realização do *design* e pela projeção da arquitetura e da implementação de elementos do sistema que cumprem os requisitos

[155] "[…] seeks to process data in such a manner that the personal data within a domain cannot be linked to the personal data in a different domain, or that establishing such a link involves a disproportionate amount of effort" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 13).

[156] "[…] ensures that it is possible for the parties involved in personal data processing, and especially the subjects whose data are processed, to intervene in the processing whenever necessary to apply corrective measures to the information processing" (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 13).

de privacidade definidos com base na centralidade do usuário (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 14-15).

As estratégias de projetos de privacidade do PbD podem ser agrupadas em duas categorias. A primeira, de natureza técnica, reúne estratégias orientadas pelo processamento dos dados (minimizar, separar, esconder e abstrair); a segunda inclui estratégias organizacionais, voltadas para a implementação de técnicas responsáveis (informar, controlar, aplicar e demonstrar) (AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2019, p. 16-17).

Figura 3 – Estratégia de projeto de privacidade.

Fonte: Elaboração da autora.

Quanto à primeira categoria, “minimizar” significa utilizar a menor quantidade de dados, evitando o processamento desnecessário para limitar possíveis impactos sobre a privacidade do usuário. Já “esconder” é limitar a observabilidade dos dados pessoais com mecanismos que garantam a proteção da confidencialidade e a desvinculação para, por meio da “abstração”, especificar os detalhes do processamento dos dados pessoais. Por fim, “separar” tem por base a divisão de informações de um usuário em processos independentes para evitar ou minimizar os riscos.

Na segunda categoria, “informar” visa a transparência na relação com a finalidade de conscientizar os usuários do processamento de seus dados pessoais, possibilitando-lhes decisões e, consequente, “controle” sobre suas informações. “Aplicar” e “demonstrar” estão relacionadas à aplicabilidade da legislação: a primeira, no sentido de verificar a compatibilidade

e o respeito aos requisitos legais; a segunda, no sentido de mostrar, tanto aos usuários quanto às autoridades de fiscalização, que o processamento de dados está seguindo os requisitos impostos pela lei.

É importante destacar o *privacy by default* – coleta e tratamento restrito. É decorrente do PbD e atende a seus princípios e metodologias:

> Considera-se que o próprio produto ou serviço deve ser arquitetado de forma condizente a proteger as informações pessoais dos seus usuários. Especificamente, por meio de uma tradução literal do termo *default*, tal desenvolvimento deveria congregar um padrão que automaticamente implementaria tal proteção com fundamento no princípio da minimização dos dados e no princípio da proporcionalidade (LIMA, 2020, p. 264).

Por meio do *privacy by default*, o sistema de informação garante um ambiente seguro para a coleta, o tratamento e a transferência de dados com base no direito à informação. O *privacy by default* capacita o usuário para controlar seus dados pessoais por meio de interfaces amigáveis. O usuário, assim, exercita sua autonomia de vontade ao controlar a proteção de seus dados pessoais. Por outro lado, o fornecedor, ao realizar uma engenharia baseada no exercício da autodeterminação informativa, possibilita a construção da confiança.

Pergunta-se: é melhor adotar uma política baseada na construção da confiança e da fidelização do cliente, na arquitetura preventiva, na segurança e no respeito aos padões de qualidade ou assumir os custos com a emissão de um relatório de impacto, com danos reputacionais e possíveis sanções pela incidência de dano ou estado de danosidade? Questiona-se aqui a formulação de uma arquitetura de rede e o estabelecimento de padrões de *design* que resultam de uma simbiose entre o direito e a tecnologia, por meio da governança, com a finalidade de efetivar comportamentos preventivos na internet. Conforme será visto na subseção seguinte, as ditas *privacy enhancing technologies* (PETs) colocam em prática a metodologia ora discutida.

5.3.2.1 *Privacy Enhancing Technologies* na concretização do *privacy by design*

Privacy enhancing technologies (PETs) são tecnologias que melhoram e reforçam a privacidade. Estão vinculadas à metodologia do *privacy by design*. São ferramentas que possibilitam o empoderamento do consumidor em relação a sua autodeterminação informacional, desempenhando “um papel multifacetado e emancipador para que o cidadão esteja, devidamente, municiado em meio à uma corrida tecnológica de vigilância, captação e mineração de dados pessoais” (BIONI, 2020a, p. 168). O *Office of the Privacy Commissioner* do Canadá assim define as PETs:

> As PETs têm como objetivo permitir que os usuários protejam sua privacidade (informativa), permitindo-lhes definir, entre outras coisas, quais informações estão dispostos a compartilhar com terceiros, como provedores de serviços *on-line*, em quais circunstâncias essas informações serão compartilhadas e com que finalidade terceiros podem usar essas informações (PRIVACY..., 2017, p. 1, tradução nossa)[157].

São exemplos de PETs a criptografia, técnicas de mascaramento de dados (ofuscação, minimização, pseudoanonimização), dados sintéticos[158] e aprendizado federado (*federated learning*)[159]. O relatório da Agência Europeia para a Segurança das Redes e da Informação Segurança (Enisa, sigla derivada do nome em inglês European Union Agency for Cybersecurity) identifica quatro categorias de PETs: mensagens seguras, redes privadas virtuais, redes anônimas e ferramentas antirrastreamento para navegação *on-line* (ENISA, 2016, p. 26).

O *Office of the Privacy Commissioner* do Canadá realizou uma divisão de PETs com base na funcionalidade de cada tecnologia, como miminização, rastreamento de dados, anonimato, controle, negociação de termos e condições, aplicação técnica[160], auditoria remota[161] e uso de direitos legais[162]:

---

[157] No original: "PETs are intended to allow users to protect their (informational) privacy by allowing them to decide, amongst other things, what information they are willing to share with third parties such as online service providers, under what circumstances that information will be shared, and what the third parties can use that information for".

[158] "Synthetic data is artificial data that is created by using different algorithms that mirror the statistical properties of the original data but does not reveal any information regarding real people" (DILMEGANI, 2020a).

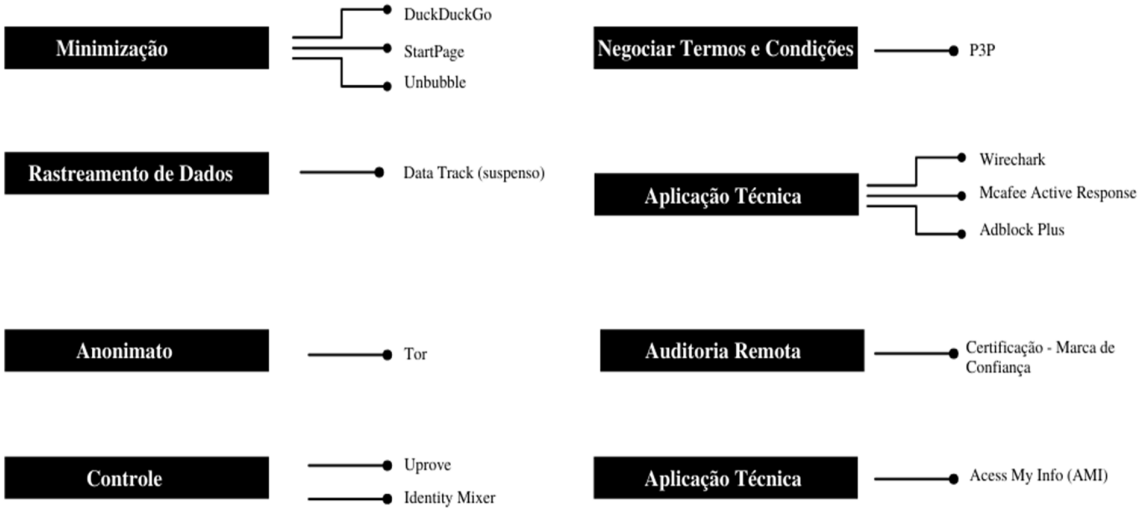
[159] "This is a machine learning technique that trains an algorithm across multiple decentralized edge devices or servers holding local data samples, without exchanging them" (DILMEGANI, 2020b).

[160] "In those instances where individuals are able to negotiate the terms and conditions of a service, PETs in this category provide individuals with the possibility of having these terms and conditions technically enforced by the infrastructures of online service providers and merchants (i.e., not just having to rely on promises, but being confident that it is technically impossible for service providers to violate the agreed upon data handling conditions)" (PRIVACY…, 2017, grifo do autor).

[161] Uma forma de "auditar" uma "marca de confiança" é verificar se o fornecedor tem uma certificação. O usuário pode averiguar se o fornecedor adota padrões de segurança em rótulos eletrônicos e representações visuais (PRIVACY…, 2017, p. 7).

[162] Formulação de uma arquitetura estrutural que possibilite o exercício de direitos garantidos na legislação, como cancelamento, retificação, entre outros.

Figura 4 – Exemplos de PETs conforme sua funcionalidade.



Fonte: Elaboração da autora.

Com relação à relativização do consentimento, as PETs podem propiciar o estabelecimento do consentimento ativo. Como ferramentas que possibilitam o consentimento verdadeiramente livre, Bioni (2020a, p. 169-176) destaca alguns projetos de tecnologias, especialmente o *Do Not Track* (DNT) (Não me rastreie) e *Platform for Privacy Preferences Project* (P3P) (Plataforma de Preferências de Privacidade). O primeiro possibilita o exercício das escolhas na coleta dos dados do consumidor, bastando "acionar o botão 'DNT' para que, automaticamente, fosse exteriorizada a sua escolha em barrar ou não a coleta de seus dados. Essa funcionalidade seria ativada pelo próprio navegador do usuário que sinaliza tal opção do usuário a todas as aplicações por ele acessadas" (BIONI, 2020a, p. 170).

A P3P, por sua vez, permite o controle e a configuração de preferências sobre a coleta de dados pessoais a partir do próprio navegador:

> Em suma, a P3P possibilitaria que o titular dos dados pessoais exercesse sobre eles um controle significativo, na medida em que tal tecnologia: i) universalizaria o processo de tomada de decisão do titular dos dados pessoais por toda a web; ii) empoderaria o titular dos dados pessoais com um poder de barganha em meio ao trade-off da economia digital, já que as preferências de privacidade seriam capazes de aumentar o leque de opções do processo de tomada de decisão sobre o fluxo informacional – consentimento granular em contraposição à lógica tudo ou nada; iii) propiciaria que, ante a automatização das escolhas dos consumidores, a autodeterminação informacional seja tão fluida quanto é o trânsito de dados pessoais; iv) possibilitaria a superação das limitações cognitivas especialmente da idiossincrasia das gratificações imediatas e perdas mediatas, já que o controle dos dados pessoais seria *ex ante* à troca pelo bem de consumo (BIONI, 2020a, p. 174-175).

É importante destacar ainda o *PrimeLife Policy Language* (PLL): baseado em XACML[163], "é usado para conceder aos provedores de serviço acesso aos dados, desde que a política da organização seja compatível com as preferências de privacidade do usuário" (PRIVACY..., 2017). Trata-se de uma estrutura dinâmica que, de um lado, quer explorar os dados e, de outro lado, quer possibilitar o exercício de um controle sobre tal manipulação (BIONI, 2020a, p. 177). É uma nítida aplicabilidade do compartilhamento da autoridade política por meio da solidariedade, tendo como base a boa-fé através dos atos coordenados entre as partes.

5.4 Regulação e *accountability* na economia de dados

As reações ao ambiente regulatório complexo da internet oferecem uma visão singular do Estado e de sua função. Keller (2019, p. 116) afirma que a regulação na internet está marcada pelo multissetorialismo por auferir representatividade as partes interessadas seja no processo de produção e execução de políticas públicas. Figura-se, assim, no reforço da legitimidade democrática pela participação ativa da sociedade no exercício da cidadania instrumental.

Para Schmidt (2012, p. 663), a legitimidade democrática na União Europeia depende de três mecanismos de legitimação: a legitimidade de insumos – referente à participação política dos cidadãos –, da legitimidade procedimental – práticas institucionais do processo de governo, como a transparência – e a legitimidade por resultado – habilidade de governar de forma efetiva. No Brasil, Keller (2019, p. 119) identifica uma relação entre a legitimidade de resultado e a exigência de eficiência da regulação "na medida em que permite um resultado informado por especificidades técnicas capazes de aumentar a aderência das políticas produzidas à realidade desses mercados" (KELLER, 2019, p. 121).

A formatação da internet é constituída por uma estrutura de governança que envolve uma pluralidade de agentes com diferentes práticas normativas e não normativas, que adotam meios não necessariamente formais para a implementação de um modelo institucional de conformidade e de negociação. A estruturação da rede on-line admite a atuação de agentes privados que impõem comportamentos.

[163] *eXtensible Access Control Markup Language* é uma arquitetura e modelo de acesso que permite ao usuário avaliar solicitações de acesso aos dados.

No Brasil, o termo "regulamentação" foi sendo progressivamente substituído por "regulação"[164] em razão dos movimentos de privatização. Regulamentação significa a produção normativa, enquanto a regulação está diretamente ligada a medidas normativas e administrativas que reconfiguram o ambiente regulado:

> A regulação, em síntese, é a presença de regras e atuação administrativa (*law and government*) de caráter conjuntural apoiadas sobre o pressuposto de diuturna reconfiguração das normas de conduta e dos atos administrativos pertinentes para a finalidade de redirecionamento constante do comportamento das atividades submetidas a escrutínio, tendo-se por norte orientador parâmetros regulatórios definidos a partir dos enunciados de atos normativos e administrativos de garantia dos direitos fundamentais (ARANHA; LOPES, 2019, p. 122).

O termo "regulação" projetou-se a partir das emendas constitucionais de 1995 e da atuação das agências reguladoras na última década do século XX e na primeira do século XXI. Além do controle e da ordenação do comportamento privado, a regulação insere-se nos princípios de direito público em conformidade com o comportamento empresarial no contexto comum (ARANHA; LOPES, 2019, p. 104-111).

Aranha e Lopes (2019, p. 150) destaca que a compreensão inovadora do direito e da regulação tem por base três pilares: a) a articulação entre as partes, assentada em uma dinâmica preventiva entre *enforcement* e *compliance*; b) a cooperação organizada; b) a centralidade da análise do custo-benefício do contexto regulado. Para a efetivação da regulação, haveria cinco estágios:

> 1) a promulgação do marco legal regulatório;
> 2) a instauração das autoridades regulatórias;
> 3) a edição de regras setoriais;
> 4) o constrangimento das condutas dos regulados para que se adaptem à normatização setorial; e
> 5) a conformidade dos regulados diante dos conteúdos das regras e das possibilidades de constrangimento, em que é possível a sua adesão autônoma aos comandos legais, como sujeitos racionais e potencialmente virtuosos (ARANHA; LOPES, 2019, p. 152).

A convergência de ações de *enforcement* e de *compliance* visam, por meio de possibilidade colaborativas, "um fim comum, que é a produção eficiente de utilidade pública, valendo-se para tanto de estratégias pedagógicas, de aconselhamento, de persuasão e de negociação, ao aplicar uma regra" (ARANHA; LOPES, 2019, p. 151). São atividades correlatas, uma vez que o *enforcement* objetiva, de um lado, a persecução e a sanção, e, de outro, a prevenção por meio da educação, do aconselhamento, da negociação, da arquitetura de

[164] "O termo 'regulação' é um desconhecido da Constituição Federal de 1988, senão por uma única referência em passagem de caráter provisório inserida pela primeira das cinco emendas constitucionais de revisão, de 1.º de março de 1994 e referente à 'regulação do Fundo Social de Emergência' instituído pela mesma Emenda Constitucional de Revisão n.º 1/1994 para os exercícios financeiros de 1994 e 1995, e disciplinado pelos arts. 71 a 73 do Ato das Disposições Constitucionais Transitórias" (ARANHA; LOPES, 2019, p. 104).

rede e do mercado, com o apoio de reguladores e regulados, todos buscando comportamentos éticos.

No que diz respeito à governança empresarial, a regulação orienta o comportamento empresarial para o cumprimento de regras pelo chamado *compliance* regulatório[165]. O comportamento social é regulado por meio do "uso de técnicas/instrumentos regulatórios informados por mecanismos de arquitetura regulatória, comandos, persuasão, abstenção, intervenção direta, contratos, prestação, fomento, fiscalização, todos eles com inteligência de incentivos, ou não" (ARANHA; LOPES, 2019, p. 184-185).

Para Defanti (2018, p. 154), são elementos essenciais do sistema regulatório: agente regulado (destinatário da atividade regulada); agente regulador (entidade que edita normas); comando (aquilo que o regulador instrui o regulado a fazer ou a abster-se de fazer); consequências (efeitos do eventual cumprimento ou descumprimento de comandos para os regulados).

A autorregulação, por outro lado, é a construção de regras comportamentais com a participação ou exclusivamente desenvolvido pelos agentes privados destinatários envolvidos na relação (ARANHA, 2019, p. 2).

Para Defanti (2018, p. 159-160), a atividade autorregulada caracteriza-se por seu caráter coletivo, regulatório mas não estatal e volitivo. Caristina (2006, p. 118-119) ressalta ainda que o modelo de autorregulação apresenta pontos específicos: a) conjunto normativo baseado nas reais necessidades dos regulados; b) maior dinâmica normativa quando comparado com a produção estatal; c) existência de organismo de supraordenação com poder de polícia, disciplinar e normativo, exercido por representante dos próprios associados. A autorregulação, portanto, induz o Estado a adotar medidas ou, simplesmente, faz com que ele reconheça o modelo já vigente.

Santanna (2011, p. 191) aponta as principais críticas ao modelo de autorregulação:

> São sintomas de ineficiência da autorregulação a ausência de transparência, tanto na formulação das normas como nas decisões em processos sancionadores; a criação de cláusulas de barreira ao ingresso na entidade ou mesmo no mercado; as dificuldades criadas para alternância de poder no âmbito da entidade; e, principalmente, a inoperância em suas funções normativa e repressiva.

No Brasil, um exemplo é o Conselho Nacional de Autorregulamentação Publicitária (Conar) criado em substituição ao regime público pretendido pelo Estado na década de 70. Entre

[165] "(…) pilares estratégicos de administração empresarial do trinômio governança-risco-compliance, mais especificamente, no que se refere ao risco operacional. Sob o enfoque da governança empresarial, o compliance regulatório consiste em estratégia empresarial frente às constrições regulatórias medida por uma análise de risco sobre a aplicação da regulamentação estatal" (ARANHA, LOPES, 2019, p. 164).

as suas competências, o Conar[166] elabora e edita o Código Brasileiro de Autorregulação Publicitária, que é norma vinculante e sancionatória para os associados, com 50 artigos e 22 anexos. Para Defanti (2018, p. 173), o Conar é um exemplo de autorregulação preventiva e espontânea, "traduzindo-se na maneira encontrada pelos agentes privados daquele setor para evitar o avanço da censura oficial sobre a atividade publicitária".

Como outros exemplos, podem-se citar o Conselho Executivo das Normas-Padrão (CENP), que edita as normas-padrão da atividade publicitária, a Bolsa de Valores e a Bolsa de Mercadorias e Futuros no mercado de capitais, entidades do mercado de balcão organizado e entidades de compensação consideradas como "órgãos auxiliares" da Comissão de Valores Mobiliários (CVM), e a Associação Brasileira de Normas Técnicas (ABNT) com chancela do poder público.

A denominação *gatekeepers* relaciona-se com "aqueles que detêm o controle sobre comportamentos, difusão e acesso à informação através da arquitetura dos sistemas utilizados para provimento de serviços" (KELLER, 2019, p. 171), cujo modelo de negócio permite a atuação conjunta com os reguladores a fim de eliminar o acesso questionável (ZITTRAIN, 2006, p. 253). Assim, tais atores são admitidos no arranjo institucional imposto na regulação da internet pela necessidade de adoção de um limite entre a regulação direta estatal e a autorregulação ou corregulação:

> O modelo de Corregulação é aquele no qual o Estado atua mediante a elaboração de normas e diretrizes gerais que asseguram uma margem de atuação e complementação por entes privados dos diversos setores da economia. Este é um formato de regulação com claros indicativos da capacidade de assegurar a harmonização entre inovação tecnológica e proteção de dados (SOMBRA, 2019, p. 73).

---

[166] De acordo com o Capítulo I do Código Brasileiro de Autorregulação Publicitária, são fundamentos da edição normativa: as diretrizes da legislação publicitária do País, especialmente capituladas na Lei n.º 4.680, de 18 de junho de 1965, e no Decreto n.º 57.690, de 1.º de fevereiro de 1966; as recomendações das Câmaras de Comércio Internacionais (ICC - International Chamber of Commerce) e as diretrizes do Código Internacional da Prática Publicitária, editado originalmente em 1937 e revisto em 1949, 1955 e 1966 e, finalmente, em 1973 durante o Congresso realizado no Rio de Janeiro e cujos termos foram adotados pelo Brasil e 250 entidades de mais de 40 países; as diretrizes da Associação Internacional de Propaganda (IAA - International Advertising Association) e seus Congressos Mundiais, especialmente as que constam de seu estudo 'Effective Advertising Self Regulation', publicado em 1974, e as recomendações do XXV Congresso Mundial de Propaganda realizado em Buenos Aires em 1976; as diretrizes do I Congresso Brasileiro de Propaganda (Rio de Janeiro, outubro de 1957), e as normas consubstanciadas no Código de Ética dos Profissionais de Propaganda então aprovadas; os termos da instrução n.º 1 da Febrasp, assinada em 23 de abril de 1968, recomendando a criação de Comissões de Ética nas entidades publicitárias; as recomendações do II Congresso Brasileiro de Propaganda (São Paulo, fevereiro de 1969), especialmente no que toca ao autopoliciamento das agências e anunciantes; as recomendações do I Encontro Nacional de Anunciantes, promovido pela ABA - Associação Brasileira de Anunciantes (São Paulo, dezembro de 1974); as recomendações feitas na I Conferência Internacional de Anunciantes (Rio de Janeiro, maio de 1975); as recomendações do simpósio realizado pela Comissão de Comunicações da Câmara dos Deputados (Brasília, junho/julho 75); - os caminhos apontados pelas lideranças do setor publicitário e pelas autoridades nos debates do II Encontro Brasileiro de Mídia, realizado em São Paulo em setembro de 1976; e as sugestões do I Seminário Brasileiro de Propaganda (Gramado, outubro de 1976) (CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA, 1980).

Segundo Aranha (2019, p. 3), a corregulação[167] é a regulação implementada pelas empresas em conjunto com Estado, ou seja, a possibilidade da intervenção estatal em caso de resultados insuficientes, pelo não cumprimento dos compromissos assumidos ou pela ameaça ao interesse público.

A corregulação é um conjunto de regras que englobam desde a criação de órgão regular até mecanismos de transparência, governabilidade e prestação de contas – *accountability*:

> Nota-se que, nesses casos, não se verifica uma partilha própria de função entre governo e agentes, ou em que a atividade dos agentes é estruturalmente sustentada por legislação. Há, isso sim, uma escolha legislativa de deixar para os prestadores de serviço a definição de uma série de critérios determinantes para a experiência do usuário, inclusive em relação ao exercício de direitos constitucionais (KELLER, 2019, p. 190).

Há um compartilhamento de competência na imposição de deveres normativos e, ao mesmo tempo, a possibilidade de implementação de procedimentos institucionais de forma cooperativa, com base nos princípios, em especial os critérios de segurança, prevenção contra riscos e prestação de contas. De acordo com o artigo 50 da LGPD, controladores e operadores, individualmente ou por meio de associações, poderão formular regras de boas práticas e governança, sob a fiscalização do Estado. Portanto, apesar do estreito enquadramento com o conceito de corregulação, existe a possibilidade de delegação, e a supervisão estatal desconfigura o modelo da corregulação.

Para Defanti (2018, p. 169), a corregulação é um tipo de autorregulação regulada. No entanto, defende-se que os dois termos designam realidades diferentes. Isso porque, como visto, a corregulação admite a intervenção estatal caso entenda pelo descumprimento das medidas estabelecidas. Já a autorregulação regulada é um mecanismo alternativo para vincular instrumentos da autorregulação a exigências públicas de transparência e *accountability*. Trata-se de um "conjunto de arranjos em que a regulação é exercida de forma primordial por agentes privados, havendo, contudo, algum tipo de supervisão ou controle estatal" (DEFANTI, 2018, p. 169). O Estado, portanto, reconhece e delega a atuação privada a determinado segmento, mantendo, porém, a possibilidade de seu controle e ratificação. Aranha e Lopes (2019, p.12) afirmam:

> A regulação manifesta-se por diversos meios, entre eles o de tecnologia de governo de sistemas sociais, que pode estar sediada em órgãos estatais – a regulação por excelência do Estado Regulador –, em mecanismos internos de controle empresarial – a metarregulação, em que o Estado audita os regimes de controle interno das

[167] A Lei Complementar n.º 137, de 2010, previu a possibilidade de corregulação no mercado de corretagem de seguros, resseguros, capitalização e previdência complementar aberta. Santanna (2011, p. 208-209) afirma: "Vale dizer, a legislação não suprimiu competências da CVM ou da Susep, apenas criou um sistema de corregulação, onde entidades por elas autorizadas funcionarão, sob sua supervisão, como auxiliares no exercício de atividades de fiscalização, julgamento e punição dos membros dos respectivos mercados".

> empresas –, em mecanismos compromissórios entre atores regulados – a corregulação –, em mecanismos institucionais privados obrigatórios – autorregulação regulada –, em mecanismos institucionais privados voluntários – autorregulação voluntária –, no vencedor do jogo político entre os atores setoriais – o livre mercado – ou, finalmente, e cada vez mais frequentemente e recomendável, em uma composição planejada de tais opções.

A autorregulação regulada – *enforced self-regulation* – é como um meio-termo entre a autorregulação e o controle, devendo a empresa produzir normas em harmonia com a preocupação do Estado, com a possibilidade de ratificação (ARANHA; LOPES, 2019, p. 22). Exige do Estado que apenas ratifique as estratégias de autorregulação:

> a) somente ratifique regras de conduta empresarial que satisfaçam as políticas públicas governamentais; b) garanta que o departamento ou grupo de compliance da empresa tenha independência na estrutura hierárquica societária; c) realize a averiguação dos livros de registro da atuação desse grupo; d) implemente fiscalizações pontuais para avaliar se o grupo está cumprindo sua finalidade de detecção de violações às normas; e e) abra processos administrativos contra empresas que tenham subvertido a atuação do grupo de compliance (ARANHA, LOPES, 2019, p. 23).

A autorregulação regulada impõe às empresas o estabelecimento de técnicas de governança e *compliance*, e as regras de conduta, podendo ser submetidas à aprovação do Estado, seu órgão regulador. Assim, o desenho regulatório cria um ambiente para que os regulados busquem boas práticas que podem ser adotadas pelo Estado. Portanto, o regulador incentiva a autorregulação em pontos específicos e adota aquelas práticas. É necessário, assim, que haja um bom ambiente institucional de comunicação entre regulador e regulado e uma agenda bem definida para que sejam estabelecidos os limites de conteúdo dessa autorregulação regulada.

Entende-se que há uma similaridade entre o arranjo institucional previsto na LGPD e a autorregulação regulada pela necessidade de cooperação entre os agentes. O compartilhamento da autoridade política é incentivado pela própria disposição institucional, regulatória e mercadológica. O Estado é, sem dúvida, ora mediador da relação ao realizar políticas públicas que ensejam a participação ativa do fornecedor, ora como agente regulado – no estabelecimento de códigos de boas práticas, em uma atuação preventiva de governança, tendo a figura estatal como órgão ratificador –, ora na condição fiscalizatória pela exigência de prestação de contas (*accountability)*.

Um exemplo concreto é a imposição da responsabilização e da prestação de contas, em observância ao artigo 6.º, X, da LGPD: “demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas”. Para Bioni (2019, p. 255), esse

princípio serve como medidor da aplicação de responsabilidade em razão da imposição de esforços para, nesse sentido, evitar a conduta danosa ou o estado de danosidade.

No entanto, a *accountability* não está restrita à exigência do Estado, diz respeito à capacidade que qualquer agente tem de impor e de requerer a prestação de contas e, consequentemente, a sanção em caso de conduta indevida no tratamento de dados:

> [...] o problema central da *accountability* envolve a delegação de autoridade a atores públicos e privados por meio da legislação, contratos ou outros instrumentos regulatórios, bem como a autonomia que a eles será concedida para que possam desempenhar suas tarefas e, ao mesmo tempo, garantir um grau adequado de controle. Confiar nos mecanismos de *accountability* é, portanto, uma pré-condição para a legitimação desse processo (SOMBRA, 2019, 187).

A *accountability* representa, nesse sentido, um meio policontextual para a tutela da privacidade e a proteção de dados pessoais por impor parâmetros claros de monitoramento em conformidade com as políticas de governança dos agentes de tratamento de dados (SOMBRA, 2019, p. 191), em atenção, inclusive, ao direito à explicação. Bioni e Luciano (2019, p. 10, grifo dos autores) afirmam:

> [...] o princípio da *accountability* apresenta-se como um vetor determinante para a *abertura* dos processos de tomadas de decisão acerca do que será considerado como um *risco tolerável* nas atividades de tratamento de dados. Isto porque a participação e o engajamento público em tais circuitos decisórios serão diretamente proporcionais ao quão elástico será o conteúdo de tal obrigação de prestação de contas por parte dos agentes econômicos. Com isso, permite-se, ao mesmo tempo, que a discussão seja porosa a valores eventualmente preteridos, uma vez experimentada a participação de atores com um outro olhar e motivados por interesses até mesmo antagônicos por parte de quem tem o dever de reportar.

Assim, o princípio da *accountability* representa um vetor de democratização da relação discutida por possibilitar a cidadania instrumental ao estabelecer o empoderamento do consumidor por meio do monitoramento dos níveis de conformidade dos dados com a legislação.

Cabe destacar o parâmetro de medida da *accountability* em atenção às hipóteses de tratamento de dados pessoais. Quanto menor a adoção dos requisitos impostos pela legislação, maior a necessidade de prestação de contas na demonstração do processamento dos dados.

Nesse sentido, é importante frisar o papel dos relatórios de impacto, um instrumento que visa "avaliar, mapear, planejar, implementar e monitorar todo o processo de conformidade com as leis gerais e setoriais de proteção de dados" (GOMES, 2019, p. 179). Trata-se de uma documentação de responsabilidade do controlador, com descrição dos processos de tratamento de dados pessoais, dos riscos para os direitos dos usuários, bem como das medidas de salvaguarda e dos mecanismos de mitigação (GOMES, 2019). Ao mesmo tempo, é um documento de governança e de prestação de contas que demonstra o nível de conformidade com

os preceitos legislativos e com as medidas de prevenção de riscos, além de indicar as possíveis sanções em caso de tratamento de dados pessoais indevido e desconforme:

> Sob a ótica do relatório de impacto sobre proteção de dados (*Privacy impact assessment*) também é possível identificar a pertinência da equação consentimento-*accountability*. Afinal, quanto maior for o risco de danos expressivos a direitos fundamentais dos titulares em virtude da operação de tratamento, mais indispensável se torna a realização de um PIA para documentar todas as atividades realizadas e as medidas mitigadoras para preservar a segurança. Os PIAs se tornaram meios relevantes de fiscalização e controle das atividades dos controladores e processadores, a partir da sua própria perspectiva, o que demonstra um olhar para as diversas variáveis envolvidas, em harmonia com a policontextualidade (SOMBRA, 2019, p. 188).

Ainda, a *accountability* estimula o *compliance* e a implementação de uma engenharia tecnológica baseada no *privacy by design* pela adoção de uma postura preventiva. Vai, portanto, além da prestação de contas em si, demonstrando as tentativas de mitigação de riscos.

A proteção de dados de consumo, portanto, tem por base um aparato normativo e estrutural que visa, ao mesmo tempo, responsabilizar e prevenir, exigindo condutas ativas de todos os agentes que compõem a relação, seja na mitigação de riscos, seja na imputação de sanções, seja no empoderamento por meio da cidadania instrumental do consumidor.

6 CONCLUSÃO

O tratamento e o uso de dados pessoais pode exercer um mecanismo de controle que irá influenciar tanto nas relações de consumo, como em todos aspectos da vida – virtual e real – do indivíduo. Assim, não existe mais a distinção entre corpo virtual e físico quando o poder no ciberespaço é exercido desde a indução de comportamento (através de técnicas como *microtargentig)* até no controle de movimentação populacional, como visto nas políticas de combate a Pandemia de Covid-19 no mundo.

É fato que a crise instaurada pela pandemia intensificou o uso de dados. Na Europa, o Projeto de Rastreamento de Proximidade de Preservação de Privacidade Pan-Europeu[168] teve por base a utilização de dados pessoais. A ideia principal é utilizar a tecnologia do *smartphone* para ajudar a interromper a onda de infecções, notificando indivíduos que tiverem em contato próximo com uma pessoa infectada - por meio do *proxy* de seus smartphones através do *Bluetooth*[169].

No que diz respeito à utilização de dados através de políticas de antipropagação do vírus, o Brasil adotou a identificação de aglomeração em cidades através de dados agregados e anonimizados por informações indicadas pelas companhias telefônicas aos Estados. Neste sentido, através de mapas de calor, identificam-se os locais com maior e menor movimentação (TALVEZ.., 2020). Mas, o grande questionamento desta política é a ausência de transparência no processo das técnicas de anonimização dos dados e, consequentemente, a impossibilidade de verificar a sua solidez de forma que inviabilize a engenharia reversa para identificação de informações pessoais. Conforme Zetter (2013), os dados anonimizados podem ser facilmente individualizados através do cruzamento de informações.

---

[168] *Pan-European Privacy-Preserving Proximity Tracing*

[169] No seu *site*, a abordagem do PEPP-PT é explicada da seguinte forma: Modo 1 - Se um usuário não for testado ou tiver seu teste indicado como negativo, o histórico de proximidade anônimo permanecerá criptografado no telefone do usuário e não poderá ser visualizado ou transmitido por ninguém. A qualquer momento, apenas o histórico de proximidade relevante para a transmissão de vírus é salvo e o histórico anterior é excluído continuamente. Modo 2 - Se o usuário do telefone A tiver sido confirmado como positivo para SARS-CoV-2, as autoridades de saúde entrarão em contato com o usuário A e fornecerão um código TAN que garante que o *malware* em potencial não possa injetar informações incorretas de infecção no sistema PEPP-PT. O usuário usa esse código TAN para fornecer voluntariamente informações ao serviço de confiança nacional que permite a notificação de aplicativos PEPP-PT registrados no histórico de proximidade e, portanto, potencialmente infectados. Como esse histórico contém identificadores anônimos para não identificar a pessoa infectada (tradução nossa) (LOMAS, 2020, p. 1, tradução livre). Vale ressaltar que empresas como *google* e *apple* estão produzindo tecnologias, como o *Bluetouth low energy*, onde o próprio aparelho identifica o contato com contaminados e informa ao usuário: "Soluções técnicas de *contact tracing* baseadas em troca de chaves e IDs aleatórios gerados por bluetooth (tecnologia de troca de contatos por proximidade), que dispensam a coleta de dados de geolocalização e identificadores únicos do dispositivo, podem ser opções de limitação ao mínimo necessário, que devem ser avaliados caso a caso" (BIONI; MONTEIRO; RIElLI, p. 18).

Nesse sentido, ousa-se afirmar que não se tem a real dimensão dos riscos advindos pelo tratamento irregular de dados pessoais, bem como, há confiança excessiva do consumidor nas plataformas eletrônicas. Consequentemente, concretiza-se as limitações do consentimento desse usuário-consumidor quando "se revela ingênuo acreditar em autonomia plena da vontade do consumidor ao, inconscientemente, transigir e dispor acerca de sua intimidade e privacidade" (VERBICARO, VIEIRA, 2021a, p. 221).

Há a vinculação da LGPD, em diálogo com o CDC, ao princípio da boa-fé objetiva, expressos, inclusive no exercício dos princípios da finalidade e da necessidade. Mas, e o consentimento? Pode-se falar no seu protagonismo? Na efetividade da autonomia de vontade nessa relação? Entende-se que não. Considerando todo esse contexto diagnosticado, busca-se formas de proteção desse consumidor em condição de vulnerabilidade e em concreto estado de danosidade.

O presente estudo apresenta uma clara divisão em sua estrutura. Os capítulos 2 e 3 visam analisar a relação de consumo que envolve o tratamento de dados pessoais, suas características e suas formas, e a utilização de dados pessoais. Um destaque é dado à publicidade direcionada, bem como ao desrespeito ao direito à vulnerabilidade-privacidade-liberdade do consumidor inserido nesse contexto. Já os capítulos 4 e 5 examinam o consentimento, buscando entender as formas de proteção do consumidor, a responsabilização por danos e a atuação conjunta visando a segurança e, especialmente, a prevenção.

No capítulo 2, foi analisada a economia de dados pessoais. Primeiramente, em uma perspectiva filosófica, para identificar a incidência da relação de poder no capitalismo informacional, cujo eixo é o consumo, alimentado pela publicidade direcionada pela modulação algorítmica. Demonstrou-se como se dá a coleta, o tratamento e a circulação dos dados pessoais para a segmentação mercadológica – *microtargeting*. Nesse processo, a publicidade direcionada é o último procedimento para modular o comportamento do consumidor, o que exige uma reestruturação da relação de consumo ante os novos agentes participantes desse ciclo.

No capítulo 3, apresentaram-se as características do consumidor inserido na economia de dados pessoais. Destacou-se a vulnerabilidade, o desrespeito à privacidade nos seus múltiplos sentidos no exercício da liberdade nas relações de consumo. Constatou-se uma assimetria relacional na vulnerabilização do consumidor inserido nesse contexto, especialmente no seu aspecto informacional, psicocomportamental, situacional e algorítmico, o que relativiza a autonomia da vontade.

No capítulo 4, aprofundou-se o consentimento, seus limites e sua função. Examinou-se o aparato legislativo brasileiro sobre a proteção de dados, ressaltando-se o Código de Defesa

do Consumidor e a Lei Geral de Proteção de Dados – que traduzem o diálogo entre as fontes. Analisou-se a observância dos direitos dos titulares de dados e dos princípios consumistas para caracterizar a responsabilidade civil por uso indevido de dados pessoais, a tutela coletiva e a incidência de dano e de um estado de danosidade quando não há consentimento ativo.

Por fim, no capítulo 5, apontaram-se os mecanismos de proteção da privacidade do consumidor além da responsabilização em si. Verificou-se que o compartilhamento da autoridade política visa não somente expandir o caráter funcional das partes, mas também possibilitar o exercício cooperativo tendo em vista o equilíbrio relacional. A própria arquitetura legislativa auxilia o compartilhamento ao impor práticas preventivas que se entrelaçam e incentivam o exercício cooperativo entre as partes.

Observou-se que o contexto da economia de dados pessoais, juntamente com as características do ambiente virtual configuram um ambiente que fragiliza o consumidor. Todo consumidor é vulnerável na relação de consumo porque há desigualdade entres as partes na relação. Constatou-se que essa condição é agravada pela possibilidade de incidência de dano e pelo estabelecimento do estado de danosidade.

Por outro lado, a autodeterminação informativa deve ser vista em uma visão ampliada, desvinculada do protagonismo do consentimento bifásico. A rede tecnológica deve possibilitar a granularidade do exercício da autonomia de vontade em todas as fases do processamento de dados. Há uma imposição legal: o usuário-consumidor deveria estar no centro protetor da relação. No entanto, há, também, uma realidade subjacente.

Não se pode negar que a legislação especial (LGPD) apresenta toda uma estrutura normativa que busca o equilíbrio, impondo ao Estado um papel primordial, seja como mediador, seja como agente central na fiscalização e na punição de fornecedores predatórios. Discute-se, porém, a sua real efetividade quando o consumidor está inserido em um mercado marcado pela insuficiência informativa e em constante evolução, a ponto do Estado não conseguir acompanhar as diárias atualizações tecnológicas.

Entende-se que a responsabilização em si pelo uso indevido de dados pessoais é de extrema importância. Mas, isso não deve ser o ponto estratégico principal na busca da proteção dos dados de consumo. Há um concreto estabelecimento da prenvenção quando se ressalta a segurança, a governança e a prestação de contas na legislação. Seria, então, a economia de dados pessoais o ambiente propício para a aplicação do princípio da prevenção para decisões automatizadas e regulatórias? Ousa-se dizer que sim em razão da estruturação de uma “zona de prevenção e proteção”.·

O princípio da prevenção tem como pilar a segurança, buscando uma nova ética de responsabilidade na antecipação de riscos ante um dano real e concreto à coletividade. Tal princípio é estabelecido na CF, que afirma, no seu artigo 5.º, que "todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros o direito à vida, à liberdade, à igualdade, à segurança e à propriedade".

Quando se analisam o CDC e a LGPD, também se observa o estabelecimento da prevenção. Por exemplo, de acordo com o artigo 6.º, I, do CDC, são direitos básicos do consumidor "a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos". Já o artigo 44 da LGPD prevê que "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes".

Na LGPD, a prevenção está ligada a diversas outras imposições porque a Lei arquiteta uma estrutura regulatória e tecnológica voltada para a proteção do usuário com base na transparência qualificada.

As arquiteturas e sistemas tecnológicos centrados na privacidade do usuário conhecidos como *privacy by design* e *privacy by default* têm como fundamento a mimização de riscos. Visam uma relação pautada pela confiança e pela fidelização do consumidor, além da preservação reputacional do fornecedor.

A governança e, consequentemente, o *compliance* seguem no mesmo sentido ao estabelecerem critérios de boas práticas para a realização de atos de prevenção e de segurança pelos fornecedores. O Estado incentiva, por exemplo, a adoção de códigos de conduta, que buscam assegurar uma relação construída com base na comunicação com os consumidores.

Para Bioni e Luciano (2019, p. 10), o princípio da *accountability* também é um vetor preventivo: expõe os riscos considerados toleráveis da atividade com possibilidade de participação e engajamento do público.

Assim, verifica-se que toda essa estruturação exige a formulação de uma relação solidária e cooperativa entre as partes. A tutela processual consumerista, como um reflexo do ideal de solidariedade e de cidadania instrumental, amplia a legitimidade, enfatiza a participação social e a proteção coletiva por meio da prática harmoniosa entre seus agentes. É inequívoco que apenas a imposição da responsabilização por dano inibe práticas mercadológicas predatórias.

Importa frisar que relações que envolvem tratamento de dados pessoais apresentam uma complexidade intrínseca. De um lado, no atual contexto de consumo cada vez mais identitário,

marcado pela mudança do padrão analógico para o digital, o consumidor tem aprimorado sua capacidade seletiva no mercado. De outro, observa-se a busca da fidelização do cliente por meio do estabelecimento de uma relação de confiança.

Não se pode esperar que, a partir da vigência da LGPD e da atuação da ANPD, o fornecedor passe a realizar condutas de boas práticas em sintonia com o que a lei exige se não existir o incentivo, tanto do Estado, na fiscalização, na autorregulação regulada ou na exigência de prestação de contas, quanto dos consumidores, no exercício da cidadania instrumental. Tudo isso requer uma configuração do pluralismo jurídico por meio do compartilhamento da autoridade política no exercício cooperativo.

Como afirmam Akerlof e Shiller (2016, p. 176), empresas podem agir unicamente em atenção ao seu benefício ou por meio do benefício compartilhado entre o seu lucro e a proteção dos consumidores. Tudo dependerá do modo como se dará o incentivo econômico, social e judicial diante de suas práticas.

O empoderamento do consumidor, o incentivo de práticas preventivas e de segurança pelo Estado, a prestação de contas e o contexto regulatório possibilitam uma ação conjunta e cooperativa entre os agentes que compõem a relação.

Especialmente quanto ao consumidor, há um concreto dilema uma vez que, ao mesmo tempo, é persuadido e luta contra ações predatórias dos fornecedores. Une-se a grupos convergentes em razão do consumo identitário, mas, por vezes, age pela influência da solidariedade mecânica porque sua inclusão ciberespacial é desqualificada.

Como forma de redução desse comportamento, é essencial que a Política Nacional de Proteção de Dados Pessoais e Privacidade defenda o consumidor e sua educação, como um princípio-diretriz, com possibilidade de participação. A Política Nacional das Relações de Consumo evidencia essa precupação ao abrir espaço para “deliberação sobre assuntos relativos à ordem de consumo” (VERBICARO, 2017, p. 538). Destaca-se ainda que a sistemática processual possibilita o exercício tanto extraprocessual quanto judicial do consumidor, em âmbito individual e coletivo, como reconhecido pela LGPD.

Ambas as Políticas devem atuar de forma conjunta e complementar, com base em ações educativas, incentivando a atuação responsável dos fornecedores e a participação política dos consumidores. É essencial a cooperação entre os órgãos que as compõem.

Não se constata a existência de uma fórmula de proteção do consumidor inserido no contexto discutido. Mas, uma estruturação relacional com o compartilhamento da autoridade entre as partes ensejará, sem dúvida, reflexos sociais. Apesar da sua inspiração na legislação consumerista, a LGPD ainda é recente para que se afirme que suas bases de segurança e de

prevenção serão, de fato, implementadas. É claro, porém, que a atuação conjunta e cooperativa gera confiança entre as partes e, consequentemente, a fidelização e a harmonia na relação. Resta-nos aguardar e observar o desenvolvimento mercadológico para descobrir quais empresas continuarão a seguir um ideal predatório e quais obterão um ganho reputacional (e, consequentemente, comercial).

REFERÊNCIAS

ABDALLA, Samuel Liló; GUESSE, André. **Informática para concursos públicos**. São Paulo: Saraiva, 2012.

ABRAMOVAY, Ricardo; ZANATTA, Rafael Augusto Ferreira. Dados pessoais abertos: pilares dos novos mercados digitais? **RDU**, Porto Alegre, v. 16, n. 90, p. 155-178, nov./dez. 2019.

A ESTRATÉGIA do Ifood com suas *push notifications*. **Inngage**, 6 out. 2019. Disponível em: https://inngage.com.br/2019/06/10/a-estrategia-do-ifood-com-suas-push-notifications/. Acesso em: 3 maio 2020.

AGAMBEN, Giorgio. **Homo Sacer**: o poder soberano e a vida nua. 2. reimpr. Belo Horizonte: UFMG, 2007. v. 1.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. **A Guide to Privacy by Design**. Espanha, Oct. 2019. Disponível em: https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf. Acesso em: 12 jun. 2021.

AKERLOF, George A.; SHILLER, Robert J. **Pescando tolos**: a economia da manipulação e fraude. Rio de Janeiro: Alta Books, 2016.

ALBUQUERQUE, Daniel. Da vulnerabilidade do consumidor à hipervulnerabilidade psíquica: ensaio sobre as raízes histórico-jurídicas e o conceito de desamparo freudiano. *In*: CARVALHO, Diógenes Faria de; FERREIRA, Vitor Hugo do Amaral; SANTOS, Nivaldo dos (org.). **Sociedade de consumo e os direitos do consumidor**. Goiânia: Editora Puc Goiás, 2014. p. 85-147.

ALVES, Amauri Cesar. Direito, trabalho e vulnerabilidade. **Revista da Faculdade de Direito UFPR**, Curitiba, v. 64, n. 2, p. 111-139, maio/ago. 2019. Disponível em: https://revistas.ufpr.br/direito/article/view/63907. Acesso em: 22 jan. 2020.

ARANHA, Marcio Iorio. As formas de autorregulação. **Jota**, 26 out. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/as-formas-de-autorregulacao-26102019. Acesso em: 20 jun. 2021.

ARANHA, Marcio Iorio; LOPES, Othon de Azevedo. **Estudo sobre teorias jurídicas da regulação apoiadas em incentivos**. Pesquisa realizada no âmbito de uma parceria da Agência Nacional de Telecomunicações com a Universidade de Brasília. Brasília, DF, 2019.

ARENDT, Hannah. **A condição humana**. 10 ed. Rio de Janeiro: Forense Universitária, 2007.

ARNAUD, André-Jean. **La gouvernance**: un outil de participation. Paris: LGDJ, 2014.

ARTICLE 29 Data Protection Working Party. Opinion 02/2010 on online behavioural advertising. Adopted on 22 June 2010. **European Commission**, 22 June 2010. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf. Acesso em: 4 maio 2020.]

ATAÍDE, Camille. **Medicalização da vida**: desafios à proteção do consumidor de saúde. São Paulo: Lumen Juris, 2020.

BAKER, Stacey Menzel. Vulnerability and Resilience in Natural Disasters: A Marketing and Public Policy Perspective. **Journal of Public Policy & Marketing**, [*s.l.*], v. 28, n. 1, p. 114-123, Spring 2009.

BAKER, Stacey Menzel; GENTRY, James W.; RITTENBURG, Terri L. Building Understanding of the Domain of Consumer Vulnerability. **Journal of Macromarketing**, [*s.l.*], v. 25, n. 2, p. 1-12, 2005.

BARASUOL JUNIOR, Orlando. **Proteção de dados pessoais**: estudo do diálogo das fontes nas relações. 2020. *E-book*.

BARBOSA, Fernanda Nunes. O dano informativo do consumidor na era digital: uma abordagem a partir do reconhecimento do direito do consumidor como direito humano. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 122, p. 203-266, mar./abr. 2019.

BARBU-KLEITSCH, Oana. Advertising, Microtargeting and Social Media. **Procedia**: Social and Behavioral Sciences, Timisoara, Romania, n. 163, p. 44-49, 2014.

BAROCELLI, Sergio Sebastián. Towards the construction of "hyper-vulnerable consumers" category. *In*: MARQUES, Claudia Lima; PEARSON, Gail; RAMOS, Fabiana (ed.). **Consumer Protection**: current challenges and perspectives. Porto Alegre: Orquestra, 2017. p. 47 – 60

BAUMAN, Zygmunt. **Globalização**: as consequências humanas. Rio de Janeiro: Zahar, 1999.

BAUMAN, Zygmunt. **Vida para consumo**: a transformação das pessoas em mercadoria. Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BAZZICALUPO, Laura. **Biopolítica**: um mapa conceitual. São Leopoldo: Editora Unisinos, 2017.

BENJAMIN, Antonio Herman V. Fato do produto e do serviço. *In*: BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. 2. ed. São Paulo: Revista dos Tribunais, 2009. p. 146-178.

BENJAMIN, Antônio Herman V.; MARQUES, Claudia Lima. A teoria do diálogo das fontes e seu impacto no Brasil: uma homenagem a Erik Jayme. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 115, p. 21-40, jan./fev. 2018.

BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor**. 5 ed. São Paulo: Revista dos Tribunais, 2013.

BIONI, Bruno Ricardo. Abrindo a "caixa de ferramentas" da LGPD para dar vida ao conceito elusivo de *privacy by design*. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito e Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 239-260.

BIONI, Bruno Ricardo. **A proteção dos dados pessoais**: a função e os limites do consentimento. 2. ed. São Paulo: Forense, 2020a.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 191-201, jan./mar. 2020b.

BIONI, Bruno Ricardo. **Xeque-mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI/USP, 2015.

BIONI, Bruno Ricardo; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, Rio de Janeiro, ano 9, n. 3, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662/506. Acesso em: 10 jan. 2021.

BIONI, Bruno Ricardo; LUCIANO, Maria. **O princípio da precaução na regulação de inteligência artificial**: seriam as Leis de Proteção de Dados o seu portal de entrada? 2019. Disponível em: https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%83O-PARA-REGULAC%CC%A7A%CC%83O-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf. Acesso em: 5 jun. 2021.

BIONI, Bruno; ZANATTA, Rafael; MONTEIRO, Renato Leite; RIELLI, Mariana. **Relatório privacidade e pandemia**: recomendações para o uso legítimo de dados no combate à COVID-19. São Paulo: Data Privacy Brasil, 2020.

BITTAR, Carlos Alberto. **Curso de direito civil**. Rio de Janeiro: Forense Universitária, 1994.

BLOTTA, Vitor Souza Lima. Privacidade e liberdade de informação em tempos de antagonismos de direitos humanos: a ladeira escorregadia para o dilema do limite legal. *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 38., 2015, Rio de Janeiro. **Anais eletrônicos** [...]. Rio de Janeiro, 2015. Disponível em: https://portalintercom.org.br/anais/nacional2015/lista_area_DT8-LE.htm. Acesso em: 3 maio 2020.

BLUM, Rita Peixoto Ferreira. **O direito à privacidade e à proteção dos dados do consumidor**. São Paulo: Almedina, 2018.

BONNA, Alexandre Pereira. Dados pessoais, identidade virtual e a projeção da personalidade: "*profiling*", estigmatização e responsabilidade civil. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). **Responsabilidade civil e novas tecnologias**. São Paulo: Editora Foco, 2020. p. 19-38.

BORGES, Fábio Mariano. **Consumerismo e consumidores indignados: negativismo contra as marcas nas redes sociais**. 2017. 154 f. Tese (Doutorado em Ciências Sociais) – Programa de Estudos Pós-Graduados em Ciências Sociais, Pontifícia Universidade Católica de São

Paulo, São Paulo, 2017. Disponível em: https://tede2.pucsp.br/handle/handle/20658. Acesso em: 17 jun. 2021.

BORGESIUS, Frederik J. Zuiderveen; MÖLLER, Judith; KRUIKEMEIER, Sanne; FATHAIGH, Ronan Ó; IRION, Kristina; DOBBER, Tom; BOBO, Balazs; VREESE, Claes de. Online Political Microtargeting: Promises and Threats for Democracy. **Utrecht Law Review**, [*s.l.*], v. 14, n. 1, p. 82-96, Feb. 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 5 jul. 2020.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 12 ago. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 7 abr. 2020.

BRASIL. **Projeto de Lei n.º 3514, de 2015**. Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9º do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2052488. Acesso em: 6 abr. 2021.

BRASIL. **Lei n.º 9.494, de 1997**. Disciplina a aplicação da tutela antecipada contra a Fazenda Pública, altera a Lei nº 7.347, de 24 de julho de 1985, e dá outras providências. Brasília, DF: Presidência da República, 1997. Disponível: http://www.planalto.gov.br/ccivil_03/leis/l9494.htm. Acesso 25 mar 2021.

BRASIL. **Lei n.º 8.429, de 1992.** Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. Brasília, DF: Presidência da República, 1992. Disponível: http://www.planalto.gov.br/ccivil_03/leis/l8429.htm Acesso 05 mar 2021.

BRASIL. **Lei n.º 4.717, de 1965.** Lei da Ação Popular. Brasília, DF: Presidência da República, 1965. Disponível: http://www.planalto.gov.br/ccivil_03/leis/l4717.htm Acesso 05 jun 2021.

BRASIL. **Lei n° 7.347, de 1985**. Lei da Ação Civil Pública. Brasília, DF: Presidência da República, 1985. Disponível: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm Acesso 06 jun 2021.

BRASIL. **Lei n.º 12.965, de 2014**. Marco Civil da Internet. Brasília, DF: Presidência da República, 2014. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso 07 jun 2021.

BRASIL. **Lei n.º 12.529, de 2011**. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica. Brasília, DF: Presidência da República, 2011. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm Acesso 07 jun 2021.

BRASIL. **Lei n° 12.414, 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, DF: Presidência da República, 2011. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm Acesso 05 jun 2021.

BRASIL. **Decreto Federal n.º 7.962, de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília, DF: Presidência da República, 2013. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm Acesso 03 jun 2021.

BRASIL. **Medida Provisória n° 954, de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, 2020. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm Acesso 04 mar 2021.

BRASIL. **Lei n° 14.181, de 2021**. Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e a Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso), para aperfeiçoar a disciplina do crédito ao consumidor e dispor sobre a prevenção e o tratamento do superendividamento. Brasília, DF: Presidência da República, 2021. Disponível: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14181.htm. Acesso 01 jul 2021.

BRASIL. **Decreto n.º 10.474, de 2020**. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança. Brasília, DF: Presidência da República, 2020. Disponível: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226 Acesso 05 jun 2021.

BRASIL. Ministério da Justiça e Segurança Pública. **Nota Técnica n.º 4/2019/GAB-SENACON/SENACON/MJ**. 2019a. Disponível em: www.justica.gov.br/news/collective-nitf-content-1555356484.15/nota-tecnica-senacon.pdf. Acesso em: 15 jan. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. **Nota Técnica n.º 32/2019/CGCTSA/DPDC/SENACON/MJ**. Processo n.º 08012.000723/2018-19. 2019b.

Disponível em: https://www.defesadoconsumidor.gov.br/portal/biblioteca/95-notas-tecnicas. Acesso em: 15 jan. 2020.

BRASIL. Ministério Público Federal; Secretaria Nacional do Consumidor; Cade; ANPD. **Recomendação**. 7 jan. 2021. Disponível em: https://www.gov.br/cade/pt-br/assuntos/noticias/cade-mpf-anpd-e-senacon-recomendam-que-whatsapp-adie-entrada-em-vigor-da-nova-politica-de-privacidade. Acesso em: 15 jun. 2021.

CALVO, Rafael A.; PETERS, Dorian; VOLD, Karina; RYAN, Richard M. Supporting Human Autonomy in AI Systems: A Framework for Ethical Enquiry. *In*: BURR, Christopher; FLORIDI, Luciano (ed.). **Ethics of Digital Well-Being**. [*S.l.*]: Springer, 2020. p. 31-54.

CANTO, Rodrigo Eidelvein do. **A vulnerabilidade dos consumidores no comércio eletrônico e a reconstrução da confiança na atualização do Código de Defesa do Consumidor**. 2014. 224 f. Dissertação (Mestrado em Direito) – Faculdade de Ciências Jurídicas e Sociais, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

CANTO, Rodrigo Eidelvein do. Direito do consumidor e vulnerabilidade no meio digital. **Revista de Direito do Consumidor**, São Paulo, v. 22, n. 87, p. 179-210, maio/jun. 2013.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 163-170, jan./mar. 2020.

CARISTINA, Jean Eduardo Aguiar. Os modelos jurídicos na auto-regulação econômica. **Prisma Jurídico**, São Paulo, v. 5, p. 113 – 131, 2006.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. **Revista de Direito do Consumidor**, São Paulo, n. 46, p. 77-119, abr./jun. 2003.

CARVALHO, Diogenes Faria de; FERREIRA, Vitor Hugo do Amaral. É solidária a responsabilidade entre aqueles que veiculam publicidade enganosa e os que dela se aproveitam na comercialização de seu produto ou serviço. *In*: MARQUES, Claudia Lima; BESSA, Leonardo Roscoe; MIRAGEM, Bruno (coord.) **Teses jurídicas dos Tribunais Superiores I**: direito do consumidor. São Paulo: Revista dos Tribunais, 2017.

CASSINO, João Francisco. Modulação deleuziana, modulação algorítmica e manipulação midiática. *In*: SOUZA, Joyce; AVELINO, Rodolfo; SILVEIRA, Sérgio Amadeu da (org.). **A sociedade de controle**. São Paulo: Hedra, 2018.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, negócios e sociedade. Rio de Janeiro: Zahar, 2015.

CASTELLS, Manuel. **A sociedade em rede**: a era da informação. 3. ed. São Paulo: Paz e Terra, 2000.

CATALA, Pierre. Ebauche d'une théorie juridique de l'information. **Informatica e Diritto**, [*s.l.*], v. 9, n. 1, p. 15-31, jan./abr. 1983.

CATALAN, Marcos. Acidentes de consumo, fato exclusivo da vítima e informação adequada e clara: um estudo de caso. **RJLB**, [*s.l.*], ano 5, n. 4, p. 1147-1172, 2019.

CATALAN, Marcos; PITOL, Yasmine Uequed. Primeiras linhas acerca do tratamento jurídico do assédio de consumi no Brasil. **Revista Luso-Brasileira de Direito do Consumo**, [*s.l.*], v. 7, n. 25, p. 137-160, mar. 2017.

CATE, Fred H; MAYER-SCHÖNBERGER, Viktor. Notice and Consent in A World of Big Data. **International Data Privacy Law**, [*s.l.*], v. 3, n. 2, p. 67-73, May 2013.

CHAZAL, Jean-Pascal. Vulnérabilité et droit de la consommation. *In*: COHET-CORDEY, Frédérique (org.). **Vulnérabilité et droit**: le développement de la vulnérabilité et ses enjeux en droit. Grenoble: Presses Universitaires de Grenoble, 2000.

COHEN, Julia E. What Privacy is for. **Harvard Law Review**, [*s.l.*], v. 126, n. 7, p. 1904-1933, 2013.

CONSELHO NACIONAL DE AUTORREGULAMENTAÇÃO PUBLICITÁRIA. Código Brasileiro de Autorregulamentação Publicitária. Maio 1980. Disponível em: http://www.conar.org.br/. Acesso em: 22 jun. 2021.

COSTA, Bárbara Regina Lopes; GONÇALVES, Rogério Antonio; MOTA, Katiuska Lorenzetti. Órgãos que garantem o que preconiza o CDC estão longe da realidade dos consumidores. **Revista Pensamento e Realidade**, [*s.l.*], v. 31 n. 2, p. 22-50, 2016.

COSTA, James Wellington Neves; OLIVEIRA, Rhenan Jandre de; LEPRE, Thais Rubia Ferreira. Perfil do consumidor 4.0 e novos modelos de negócio. **South American Development Society Journal**, [s.l.], v. 5, n. 15, p. 499-516, 2020.

COTS, Márcio; OLIVEIRA, Ricardo de (coord.). **O legítimo interesse e a LGPDP**. São Paulo: Revista dos Tribunais, 2020.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: Internet Users'Understanding of Behavioral Advertising. **TPRC**, Schertz, TX, p. 1-31, 2010. Disponível em: http://ssrn.com/abstract=1989092. Acesso em: 30 maio 2020.

CUSTERS, Bart; VAN DER HOF, Simone; SCHERMER, Bart; APPLEBY-ARNOLD, Sandra; BROCKDORFF, Noellie. Informed Consent in Social Media Use: The Gap between User Expectations and EU Personal Data Protection Law. **SCRIPTed**, [*s.l.*], v. 10, n. 4, p. 435-457, 2013.

DEFANTI, Francisco. Um ensaio sobre a autorregulação: características, classificações e exemplos práticos. **Revista de Direito Público da Economia**, Belo Horizonte, ano 16, n. 63, p. 149-181, jul./set. 2018.

DE LA BOÉTIE, Étienne. **Discurso sobre a servidão voluntária**. Lisboa: Antígona, 2016.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. *In*: DELEUZE, Gilles. **Conversações**. Rio de Janeiro: Editora 34, 1992. p. 219-226.

"DEUS não morreu. Ele tornou-se Dinheiro". Entrevista com Giorgio Agamben. Entrevistador: Peppe Salvà. Tradução de Selvino J. Assmann. **Instituto Humanas Unisinos**, 30 ago. 2012. Entrevista. Disponível em: http://www.ihu.unisinos.br/noticias/512966-giorgio-agamben. Acesso em: 10 jul. 2019.

DIDIER JR., Fredie; ZANETI JR., Hermes. **Curso de direito processual civil**: processo coletivo. Salvador: JusPODIVM, 2017. v. 4.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. São Paulo: Revista dos Tribunais, 2019.

DUHIGG, Charles. **O poder do hábito**: por que fazemos o que fazemos na vida e nos negócios. Tradução de Rafael Mantovani. Rio de Janeiro: Objetiva, 2012.

EFING, Antônio Carlos; CAMPOS, Fábio Henrique Fernandez de. A vulnerabilidade do consumidor em era de ultramodernidade. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 115, p. 149-165, jan./fev. 2018.

ENISA. **Privacy Enhancing Technologies**: Evolution and State of the Art A Community Approach to PETs Maturity Assessment. Dec. 2016.

ENRIQUEZ, Eugène. L'idéal type de l'individu hypermoderne: l'individu pervers? *In*: AUBERT, Nicole (org). **L'individu hypermoderne**. Toulouse: Érès, 2004. p. 51-80.

FACHINI, Elaine Cristina Sotelo; FERRER, Walkiria Martinez Heinrich. Biopolítica e biopoder como forma de intervenção na origem econômica e de controle social: a lei geral de proteção de dados como inibitória da manipulação social. **Revista Direito UFMS**, Campo Grande, MS, v. 5, n. 2, p. 226-246, jul./dez. 2019.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de direito civil**: contratos: teoria geral e contratos em espécie. 3. ed. Salvador: JusPODIVM, 2013.

FEDERAL TRADE COMMISSION. Bureau of Consumer Protection. **Online Profiling:** A Report to Congress. Washington, DC, June 2000. Disponível em: https://www.ftc.gov/system/files/documents/reports/online-profiling-federal-trade-commission-report-congress-june-2000/onlineprofilingreportjune2000.pdf. Acesso em: 2 maio 2020.

FEDERAL TRADE COMMISSION. **Data Brokers**: A Call for Transparency and Accountability. Washington, DC, May 2014. Disponível em: https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014. Acesso em: 30 maio 2020.

FERRAÇO, André Augusto Giuriatto. A autodeterminação informativa do consumidor a partir da proteção de dados no âmbito internacional. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 125, p. 167-194, set./out. 2019.

FERREIRA, Jussara Suzi Assis Borges Nasser; ROSA, André Luís Cateli. Fornecimento eletrônico de dados pessoais dos consumidores: responsabilidade civil objetiva e solidária e o

dano social. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 122, p. 233-266, mar./abr. 2019.

FERREIRA, Rafael Freire. **Autodeterminação informativa e a privacidade na sociedade da informação**. 4. ed. São Paulo: Lumen Juris, 2019.

FISHER, Luciana. Revista propaganda: a publicitária na mídia segmentada (um estudo de caso). *In*: CONGRESSO BRASILEIRO DE CIÊNCIAS DA COMUNICAÇÃO, 24., Campo Grande, MS, 2001. **Anais eletrônicos** [...], Campo Grande, 2001. Disponível em: http://www.intercom.org.br/papers/nacionais/2001/papers/NP3FISCHER.PDF. Acesso em: 5 mar. 2021.

FONSECA, Aline Klayse dos Santos. **Responsabilidade civil**: do dano à danosidade. Rio de Janeiro: Lumen Juris, 2019.

FORTES, Vinicius Borges. **Os direitos de privacidade e a proteção de dados na internet**. São Paulo: Lumen Juris, 2016.

FOUCAULT, Michel. **Microfísica do poder**. Tradução de Roberto Machado. 2. ed. Rio de Janeiro: Paz e Terra, 2015.

FOUCAULT, Michel. **Nascimento da biopolítica**. Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Vigiar e punir**: o nascimento da prisão. Tradução de Raquel Ramalhete. 20 ed. Petrópolis: Vozes, 1999.

FRAGA, Vitor Galvão. O Direito das obrigações e o paradigma da confiança. Revista **Revista Jurídica da Seção Judiciária de Pernambuco,** Recife, n; 10, p. 419-446, 2017.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters, 2019. p. 677-715.

FREIRE, Gabriela Ohana Rocha. **O empoderamento virtual do consumidor como mecanismo de atuação cívica on-line indutor de novos padrões ao segmento empresarial**. 2020. 218 f. Dissertação (Mestrado em Direito) – Universidade Federal do Pará, Belém, 2020.

FREITAS, Arystóbulo de Oliveira. A publicidade inserida na relação de consumo. **Revista do Instituto dos Advogados de São Paulo**, São Paulo, v. 1, n. 1, p. 18-27, jan./jun. 1998.

FREITAS, Cinthia Obladen de Almendra; MAFFINI, Maylin. A proteção dos dados pessoais no crédito bancário e a lei geral de proteção de dados frente ao cadastro positivo. **Revista Jurídica Cesumar**, Maringá, PR, v. 20, n. 1, p. 29-42, jan./abr. 2020.

GARCIA, Gustavo Filipe Barbosa. **Manual de direito do trabalho**. São Paulo: Método, 2012.

GARCIA, Leonardo de Medeiros. O princípio da informação na pós-modernidade: direito fundamental do consumidor para o equilíbrio nas relações de consumo. **Revista Direito**

Unifacs, Salvador, n. 176, 2015. Disponível em: https://revistas.unifacs.br/index.php/redu/issue/view/208. Acesso em: 30 maio 2020.

GAVRONSKI, Alexandre Amaral. **Técnicas extraprocessuais de tutela coletiva**. São Paulo: Revista dos Tribunais, 2010.

GOGONI, Ronaldo. Facebook admite que monitora automaticamente todas as conversas do Messenger. **MeioBit**, 5 abr. 2018. Disponível em: https://www1.tecnoblog.net/meiobit/382682/facebook-messenger-rede-social-verifica-conteudo-automaticamente-atras-mensagens-violando-termos-servico/. Acesso em: 4 maio 2020.

GOLDSCHMIDT, Ronaldo; BEZERRA, Eduardo. Exemplos de aplicações de data mining no mercado brasileiro. **ComputerWorld**, 27 jun. 2016. Disponível em: https://computerworld.com.br/2016/06/27/exemplos-de-aplicacoes-de-data-mining-no-mercado-brasileiro/. Acesso em: 2 maio 2020.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados pessoais. **Revista do Advogado**, Rio de Janeiro, ano 39, n. 144, p. 174-183, nov. 2019.

GOOGLE é condenada a indenizar homem que apareceu em Street View. **Tecmundo**, 8 jul. 2015. Disponível em: https://www.tecmundo.com.br/google/82898-google-condenada-indenizar-homem-apareceu-street-view.htm. Acesso em: 15 mar. 2021.

GRINOVER, Ada Pellegrini *et al*. **Código Brasileiro de Defesa do Consumidor**. 6. ed. São Paulo: Forense Universitária, 1999.

HAN, Byung-Chul. O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han. **El País**, 22 mar. 2020. Disponível em: https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-amanha-segundo-o-filosofo-byung-chul-han.html. Acesso em: 26 mar. 2020.

HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Belo Horizonte: Âyiné, 2018.

HARVEY, David. **A produção capitalista do espaço**. São Paulo: Annablume, 2005.

HOMO oeconomicus, de Foucault, e animal laborans, de Arendt: conceitos para pensar o tempo presente. Entrevistado: Adriano Correia Silva. Entrevistadores: Márcia Junges e Leslie Chaves. **Revista do Instituto Humanitas Unisinos on-line**, Porto Alegre, edição 468, 29 jun. 2015. Disponível em: http://www.ihuonline.unisinos.br/artigo/6023-adriano-correia-1. Acesso em: 20 maio 2020.

HOOFNAGLE, Chris Jay; URBAN, Jennifer M.; LI, Su. Privacy and Modern Advertising: Most US Internet Users Want 'Do Not Track' to Stop Collection about their Online Activities. **Amestedam Privacy Conference**, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2152135. Acesso em: 30 maio 2020.

HOW Dark Patterns Trick You Online. Produção de Nerdwriter1. 2018. 1 vídeo (ca 7 min). Disponível em: https://www.youtube.com/watch?v=kxkrdLI6e6M. Acesso em: 3 abr. 2021.

JOELSONS, Marcela. O legítimo interesse do controlador no tratamento de dados pessoais e o teste de proporcionalidade europeu: desafios e caminhos para uma aplicação no cenário brasileiro. **Revista de Direito e as Novas Tecnologias**, São Paulo, n. 8, jul./set. 2020.

JOVANELLE, Valquíria de Jesus. **Aspectos jurídicos dos contratos eletrônicos**. 2012. 133 f. Dissertação (Mestrado em Direito) – Universidade de São Paulo, São Paulo, 2012.

KALBACH, Jim. **Mapeamento de experiências**. Rio de Janeiro: Alta Books, 2017.

KELLER, Clara Iglesias. **Regulação nacional de serviços da internet**: exceção, legitimidade e o papel do Estado. São Paulo: Lumen Juris, 2019.

KLAFKE, Guilherme Forma. **Como um voto no BBB21 pode gerar criptoativos? Sobre** paredões e smart contracts**.** ***Medium****, 20 abr. 2021. Disponível em:* https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/como-um-voto-no-bbb21-pode-gerar-criptoativos-sobre-pared%C3%B5es-e-smart-contracts-3ce1d735e5a7. *Acesso em: 2 maio 2021.*

KONDER, Carlos Nelson de Paula; SOUZA, Amanda Guimarães Cordeiro de. Onerosidade do acesso às redes sociais. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 121, p. 185-212, jan./fev. 2019.

KONDER, Carlos Nelson de Paula. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. **Revista de Direito do Consumidor**. São Paulo, v. 24, n. 99, p. 101 – 123, maio-jun, 2015.

KOZLOVSKI, Aline Chamié. O controle da oferta excessiva pelos meios eletrônicos e a velocidade das contratações no mercado de consumo. *In*: VERBICARO, Dennis; ATAÍDE, Camille; ACIOLI, Carlos (coord.). **Provocações contemporâneas no direito do consumidor.** Rio de Janeiro: Lumen Juris, 2018. p. 115-146.

KRUG, Steve. **Não me faça pensar**: uma abordagem de bom senso à usabilidade na web e mobile. Rio de Janeiro: Alta Books, 2014.

LACE, Susanne. **The glass consumer**: life in a surveillance society. Bristol: Bristol University Press, 2005.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LEONARDI, Marcel. Principais Bases Legais de Tratamento de Dados Pessoais no Setor privado. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito e Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 317 – 332.

LESSIG, Lawrence. **Code**: Version 2.0. [*S.l.*]: Basic Books, 2006.

LÉVY, Pierre. **As tecnologias da inteligência**: o futuro do pensamento na era da informática. São Paulo: Editora 34, 1993.

LEVY, Steven. Secret of Googlenomics: Data-Fueled Recipe Brews Profitability. **Wired**, 22 maio 2009. Disponível em: https://www.wired.com/2009/05/nep-googlenomics/. Acesso em: 3 jun. 2020.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados**. São Paulo: Almedina, 2020.

LIMA, Cíntia Rosa Pereira de. Consentimento inequívoco *versus* expresso: o que muda com a LGPD? **Revista do Advogado**, Rio de Janeiro, ano 39, n. 144, p. 60-66, nov. 2019.

LIMBERGER, Têmis; SALDANHA, Jânia; HORN, Luiz Fernando Del Rio. Do dilema paradoxal tecnocívico: inclusão consumerista digital qualitativa versus qualitativa. **Revista de Direito do Consumidor**, São Paulo, v. 26, n. 114, p. 195-226, nov./dez. 2017.

LIPOVETSKY, Gilles. **A felicidade paradoxal**: ensaio sobre a sociedade do hiperconsumo. Tradução de Maria Lucia Machado. São Paulo: Companhia das Letras, 2007.

LOMAS, Natasha. An EU Coalition of Techies Is Backing A 'Privacy-Preserving' Standard for COVID-19 Contacts Tracing. **TechCrunch**, April 1, 2020. Disponível em: https://techcrunch.com/2020/04/01/an-eu-coalition-of-techies-is-backing-a-privacy-preserving-standard-for-covid-19-contacts-tracing/. Acesso em: 17 abr. 2020.

LONGO, Walter. **Marketing e comunicação na era pós-digital**: as regras mudaram. São Paulo: HSM do Brasil, 2014.

LOPES, Maria Elizabete Vilaça. O consumidor e a publicidade. **Doutrinas Essenciais de Responsabilidade Civil**, São Paulo, v. 4, p. 949-982, out. 2011.

LORENZETTI, Ricardo Luis. **Comércio eletrônico**. São Paulo: Revista dos Tribunais, 2004.

LOVELUCK, Benjamin. **Redes, liberdade e controle**: uma genealogia política da internet. Petrópolis: Vozes, 2015.

LOWDERMILK, Travis. **Design centrado no usuário**: um guia para o desenvolvimento de aplicativos amigáveis. São Paulo: Novatec Editora, 2013.

LUCCA, Newton de. **Aspectos jurídicos da contratação informática e telemática**. São Paulo: Saraiva, 2003.

LUCCA, Newton de; LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. Cap. 15.

MALCHER, Farah de Sousa; DELUCHEY, Jean-François Yves. A origem biopolítica do direito tributário. **Revista Brasileira de História do Direito**, Curitiba, v. 2, n. 2, p. 39-59, jul./dez. 2016.

MALHEIRO, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet**: uma análise comparada do Regulamento Geral de Proteção de Dados europeu e do Projeto de Lei 5.276/2016. 2017. 86 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, DF, 2017.

MARCACINI, Augusto Tavares Rosa. Considerações sobre a proteção à privacidade e aos dados pessoais em uma sociedade digital. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito e Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 129-146.

MARQUES, Claudia Lima. Diálogo entre o Código de Defesa do Consumidor e o novo Código Civil: do diálogo das fontes no combate às cláusulas abusivas. **Revista de Direito do Consumidor**, v. 45, p. 71-99, jan/mar. 2003.

MARQUES, Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor**. São Paulo: Revista dos Tribunais, 2004a.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor**: o novo regime das relações contratuais. 6. ed. São Paulo: Revista dos Tribunais, 2011.

MARQUES, Cláudia Lima. Superação das antinomias pelo diálogo das fontes: o modelo brasileiro de coexistência entre o Código de Defesa do Consumidor e o Código Civil de 2002. **Revista da Escola Superior da Magistratura de Sergipe**, Aracaju, n. 7, p. 15-54, 2004b.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. São Paulo: Revista dos Tribunais, 2012.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e *compliance*. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. cap. 14.

MATTIA, Fabio Maria de. Direitos da personalidade: aspectos gerais. **Doutrinas Essenciais de Direito Civil**, São Paulo, v. 3, p. 245-268, out. 2010.
MATTIA, Fabio Maria de. Direitos da personalidade: aspectos gerais. **Revista Forense**, Rio de Janeiro, v. 74, n. 262, p. 79-88, abr./jun. 1978.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais: novo direito fundamental precisará ter contornos definidos tanto pela jurisprudência, quanto pela doutrina. **Jota**, 10 maio 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 15 maio 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva Jur, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020.

MENDIETA, Ezequiel N. Towars Tourists Protection in the Digital Age. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 124, p. 139-156, jul./ago. 2019.

MILHOMENS, Heitor Antunes. **Tutela da confiança e da vulnerabilidade na economia do compartilhamento**: empoderamento do consumidor digital e mitigação da vulnerabilidade estrutural na era do hiperconsumo. 2021. 228 f. Dissertação (Mestrado em Direito) – Universidade Federal do Pará, Belém, 2021.

MILLER, Geoffrey. **Darwin vai às compras**: sexo, evolução e consumo. 2. ed. Rio de Janeiro: BestSeller, 2012.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. **Revista dos Tribunais**, São Paulo, v. 108, n. 1009, p. 173-222, nov. 2019a.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 6. ed. São Paulo: Revista dos Tribunais, 2016.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 125, p. 17-62, set./out. 2019b.

MIRAGEM, Bruno. **Responsabilidade civil**. 2. ed. Rio de Janeiro: Forense, 2021.

MITSUICHI, Lucas. Big data: conheça os 5 V's e sua aplicação prática para PMEs. **SEMRUSH Blog**, 19 fev. 2020. Disponível em: https://pt.semrush.com/blog/big-data-conheca-os-5-vs-e-sua-aplicacao-pratica-para-pmes/. Acesso em: 7 maio 2020.

MORASSUTTI, Bruno Schimitt. Responsabilidade civil, discriminação ilícita e algoritmos computacionais: breves estudos sobre as práticas de geoblocking e geopricing. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 124, p. 213-234, jul./ago. 2019.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e consentimento na Lei Geral de Proteção de Dados Pessoais. **Revista do Advogado**, Rio de Janeiro, ano 39, n. 144, p. 47-53, nov. 2019.

NISSENBAUM Helen. Privacy as contextual integrity. ***Washington Law Review***, Washington, DC, v. *79*, *n.* 1, p. 119-157, 2004.

NUNES, Rizzatto. **Curso de direito do consumidor**. 11. ed., rev. e atual. São Paulo: Saraiva, 2017.

OLIVEIRA, Amanda Flávia de; CARVALHO, Diógenes Faria de. Vulnerabilidade comportamental do consumidor: porque é preciso proteger a pessoa superendividada. **Revista de Direito do Consumidor**, São Paulo, v. 25, n. 104, p. 181-201, mar./abr. 2016.

OLIVEIRA, Priscilla. 3 tipos de cancelamentos que uma marca pode sofrer. **Mundo do Marketing**. 23 set 2020. Disponível https://www.mundodomarketing.com.br/reportagens/comportamento-do-consumidor/38869/3-tipos-de-cancelamentos-que-uma-marca-pode-sofrer.html Acesso 04 jun 2021

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**: Como o Big Data aumenta a desigualdade e ameaça a democracia. Santo André, São Paulo: Ed. Rua do Sabão, 2020.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICOS. **Síntese**: Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais. [*S.l.*]: OCDE, 2002.

PAIXÃO, Adrian Gabriel Fideles; KAI, Bruna Teixeira. Direito do patrimônio cultural na era da informação: bens digitais e a tutela jurídica. **RIHGRGS**, Porto Alegre, n. 157 especial, p. 209-230, abr. 2020.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen de Almendra; MEIRELES, Jussara Maria Leal de. Vicio do consentimento através do neuromarketing nos contratos da era digital. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 115, p. 331-356, jan./fev. 2018.

PIMENTA, Joaquim. Autonomia de vontade e dirigismo contratual. **Revista do Serviço Público**, [*s.l.*], v. 78, n. 1, 2 e 3, p. 131-135, jan./fev./mar. 1958.

PODESTÁ, Fabio Henrique. A privacidade e o consentimento (informado) em face da nova Lei de Proteção de Dados. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito e Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 81-104.

POLÍTICA de Privacidade e de Proteção de Dados da Lojas Renner S.A. **RENNER**, última atualização em 27 ago. 2020. Disponível em: https://www.lojasrenner.com.br/privacidade-seguranca. Acesso em: 7 dez. 2020.

PRIVACY Enhancing Technologies: A Review of Tools and Techniques. **Office of The Privacy Commissioner of Canada**, November 2017. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. Acesso em: 13 jun. 2021.

QUAL é a diferença entre Business Intelligence e Big Data? **Blog da Five Acts**, 27 nov. 2020. Disponível em: https://www.fiveacts.com.br/afinal-qual-diferenca-entre-business-intelligence-e-big-data/. Acesso em: 7 dez. 2020.

QUINTARELLI, Stefano. A revolução digital e transformações sociais. Tradução de Rodrigo Bravo. **DOWBOR.ORG**, 1 fev. 2019. Disponível em: https://dowbor.org/2019/02/stefano-quintarelli-a-revolucao-digital-e-transformacoes-sociais-fev-2019-10p.html/. Acesso em: 7 maio 2020.

RASLAN, Daniela Andrade; CALAZANS, Angélica Toffano Seidel. *Data Warehouse*: conceitos e aplicações. **Universitas Gestão e TI**, Brasília, DF, v. 4, n. 1, p. 25-37, jan./jun.

2014.

RIBAS, Mariana. Senacon notifica Rappi para explicar coleta de dados dos clientes. **Jota**, 10 jan. 2020. Disponível em: https://www.jota.info/jotinhas/rappi-senacon-dados-10012020. Acesso em: 24 mar. 2021.

ROCHA, Luiz Alberto G. S. A dimensão constitucional da proteção do consumidor no Brasil e o desafio da formação do consumidor reflexivo. *In*: VERBICARO, Dennis; ATAÍDE, Camille; ACIOLI, Carlos (coord.). **Provocações contemporâneas no direito do consumidor**. Rio de Janeiro: Lumen Juris, 2018. p. 1-22.

ROCHA, Luiz Alberto G. S.; MAZIVIERO, Luiza Nobre. Por um click: como a Lei Geral de Proteção de Dados Pessoais possibilita o "consentimento involuntário" de fornecimento de informações de particulares a empresas. *In*: VERBICARO, Dennis; VERBICARO, Loiane; VIEIRA, Janaina (org.). **Direito do consumidor digital**. São Paulo: Lumen Juris, 2020. p. 3-24.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Lays Soares dos Santos. **Precisamos falar sobre o assédio de consumo**: a publicidade a serviço da indústria cultural. Rio de Janeiro: Lumen Juris, 2019.

RODRÍGUEZ-GARAVITO, César. Beyond the Courtroom: The Impact of Judicial Activism on Socioeconomic Rights in Latin America. **Texas Law Review**, [*s.l.*], n. 89, p. 1669-1698, 2011.

ROQUE, André. A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Eletrônica de Direito Processual**, Rio de Janeiro, ano 13, v. 20, n. 2, p. 1-19, maio/ago. 2019.

ROSA, Natalie. Google deve pagar multa de US$ 13 milhões por polêmica Wi-Spy de coleta de dados. **Yahoo Finanças**, 22 jul. 2019. Disponível em: https://br.financas.yahoo.com/noticias/google-deve-pagar-multa-us-210000555.html. Acesso em: 15 mar. 2021.

SALLES, Carlos Alberto de. Processo civil de interesse público. *In*: SALLES, Carlos Alberto de (org). **Processo civil e interesse público**: o processo como instrumento de defesa social. São Paulo: Revista dos Tribunais, 2003. p. 39-77.

SÁNCHEZ-OCAÑA, Alejandro Suárez. **A verdade por trás do *Google***: a inquietante realidade que não querem que você conheça. Tradução de Sandra Martha Dolinsky. São Paulo: Planeta, 2013.

SANTANNA, Luciano Portal. Autorregulação supervisionada pelo Estado: desenvolvimento de um sistema de corregulação para o mercado de corretagem de seguros, resseguros, capitalização e previdência complementar aberta. **Revista de Direito Administrativo**, Rio de Janeiro, v. 257, p. 183-211, maio/ago. 2011.

SANTIAGO, Mariana Ribeiro; ANDRADE, Sinara Lacerda. A obsolescência programada e psicológica como forma de biopoder: perspectivas jurídicas do consumismo. **Quaestio Juris**, Rio de Janeiro, v. 9, n. 4, p. 1771-1786, 2016.

SANTOS, Boaventura de Sousa. **A crítica da razão indolente**: contra o desperdício da experiência. 2. ed. Porto: Edições Afrontamento, 2002.

SANTOS, Boaventura de Sousa. **Reconhecer para libertar: os caminhos do cosmopolitanismo multicultural.** Rio de Janeiro: Civilização Brasileira, 2003.

SARLET, Ingo Wolfgang; MOLINARO, Carlos Alberto. Direito à informação e direito ao acesso à informação como direito fundamentais na Constituição brasileira. **Revista da AGU**, Brasília, DF, ano XIII, n. 42, p. 9-38, out./dez. 2014.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2018.

SCHMIDT NETO, André Perin. **Contratos na sociedade de consumo**: vontade e confiança. São Paulo: Revista dos Tribunais, 2016.

SCHMIDT, Vivien A. Democracy and Legitimacy in the European Union. In: JONES, Erik; MENON, Anand; WEATHERILL, Stephen. **The Oxford Handbook of the European** Union. Oxford: Oxford University Press, 2012. p. 661-675.

SCHMITT, Carl. Definition of Sovereignty. *In*: SCHMITT, Carl. **Political Theology**: Four Chapters on the Concept of Sovereignty. Chicago: University of Chicago Press, 2005.

SCHREIBER, Anderson. Contratos eletrônicos no direito brasileiro: formação dos contratos eletrônicos e direito de arrependimento. *In*: MELGARÉ, Plínio (org.). **Direito das obrigações na contemporaneidade**: estudos em homenagem ao Ministro Ruy Rosado de Aguiar Júnior. Porto Alegre: Livraria do Advogado, 2014. p. 41-60. Disponível em: http://www.andersonschreiber.com.br/downloads/artigocontratos-eletronicos.pdf. Acesso em: 25 mar. 2021.

SCHREIBER, Anderson. Contratos Eletrônicos e Consumo. **Revista Brasileira de Direito Civil**, São Paulo, v. 1, p. 88-110, jul /set, 2014b.

SILVA, Bruno Anderson Souza da. **A profanação do improfanável**: o "capitalismo como religião" e uma reflexão ética a partir de Agamben. [*S.l.*]: Editora Fi, 2018.

SIMÃO, Bárbara; OMS, Juliana; TORRES, Lívia. **Autoridades de proteção de dados na América Latina**: um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. São Paulo: IDEC, 2019.

SIMÃO FILHO, Adalberto. A governança corporativa aplicada às boas práticas e *compliance* na segurança de dados. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. cap. 13.

SOLOMON, Michael R. **O comportamento do consumidor**: comprando, possuindo e sendo. 9. ed. Porto Alegre: Bookman, 2011.

SOLOVE, Daniel J. Introduction: Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, Cambridge, MA, v. 126, n. 7, p. 1880-1903, May 2013.

SOMBRA, Thiago Luís Santos. **Direito á privacidade e proteção de dados pessoais no ciberespaço:** a accountability como fundamento da Lex Privacy. 2019. 219 f. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, DF, 2019.

STEVEN JOBS: "There's sanaty retorning". **Bloomberg Businessweek**. 25 maio de 1998. Disponível em https://www.bloomberg.com/news/articles/1998-05-25/steve-jobs-theres-sanity-returning Acesso em 5 jun 2021.

'TALVEZ seja necessário demonstrar boa saúde para viajar por meio de aplicativo após Covid-19'. **Estúdio CBN**, 17 abril 2020. Disponível em: https://m.cbn.globoradio.globo.com/media/audio/298593/talvez-apos-covid-19-seja-necessario-demonstrar-es.htm. Acesso em: 18 abr. 2020.

TAMA, Adhi Bayu. Data Mining for Predicting Customer Satisfaction in Fast-Food Restaurant. **Journal of Theoretical and Applied Information Technology**, [*s.l.*], v. 75, n. 1, p. 18-24, May 2015. Disponível em: http://www.jatit.org/volumes/seventyfive1.php. Acesso em: 2 maio 2020.

TASSO, Fernando Antonio. responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, ano 21, n. 53, p. 97-116, jan./mar. 2020.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Responsabilidade e ressarcimento de danos por violações às regras previstas na LGPD: um cotejamento com o CDC. *In*: LIMA, Cíntia Rosa Pereira de (coord.). **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. cap. 12.

TERMOS de serviço do Google. Versão específica: Brasil. **Google**, 31 mar. 2020. Disponível em: https://policies.google.com/terms?hl=pt-BR. Acesso em: 3 maio 2020.

THEODORO JÚNIOR, Humberto; NUNES, Dierle; BAHIA, Alexandre Melo Franco. Litigância de interesse público e execução comparticipada de políticas públicas. **Revista de Processo**, São Paulo, v. 38, n. 224, p. 121-153, out. 2013.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. ***Jornal Oficial das Comunidades Europeias***, C326/02, 26 out. 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT. Acesso em: 5 abr. 2021.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias**, L281, p. 31-50, 23 nov. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 5 abr. 2021.

UNIÃO EUROPEIA. Directiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de maio de 2005. Relativa às práticas comerciais desleais das empresas face aos consumidores

no mercado interno e que altera a Directiva 84/450/CEE do Conselho, as Directivas 97/7/CE, 98/27/CE e 2002/65/CE e o Regulamento (CE) n.º 2006/2004. **Jornal Oficial da União Europeia**, L149, 11 jun. 2005. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32005L0029&qid=1625930712136. Acesso em: 5 abr. 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, L119, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/pt/TXT/?qid=1559291025147&uri=CELEX:32016R0679#d1e1564-1-1. Acesso em: 5 abr. 2021.

UNIÃO EUROPEIA. Regulamento (UE) 2018/302 do Parlamento Europeu e do Conselho, de 28 de fevereiro de 2018. Visa prevenir o bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade, no local de residência ou no local de estabelecimento dos clientes no mercado interno, e altera os Regulamentos (CE) n.º 2006/2004 e (UE) 2017/2394 e a Diretiva 2009/22/CE. **Jornal Oficial da União Europeia**, L60, p. 1-15, 2 mar. 2018. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32018R0302. Acesso em: 5 abr. 2021.

U.S. DEPARTMENT OF HEALTH, EDUCATION & WELFARE. **Records, Computers and the Rights of Citizens**. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, DC, July 1973.

VALIM, Thalles Ricardo Alciati. Natureza jurídica e formação dos contratos eletrônicos. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 123, p. 251-288, maio/jun. 2019.

VAN DEN HOVEN, Jeroen; BLAAUW, Martijn; PIETERS, Wolter; WARNIER, Martijn. Privacy and Information Technology. *In*: ZALTA, Edward N. (ed.). **The Stanford Encyclopedia of Philosophy**. Summer Edition, 2020. Disponível em: https://plato.stanford.edu/archives/sum2020/entries/it-privacy/. Acesso em: 5 abr. 2021.

VERBICARO, Dennis. A liberdade humana sob a perspectiva anarquista é uma diretriz para a sociedade pós-moderna. **Revista da Procuradoria Geral do Estado do Pará**, v. 17, p. 63-93, 2007.

VERBICARO, Dennis. A política nacional das relações de consumo como modelo de democracia deliberativa. **Revista Jurídica da Presidência**, Brasília, DF, v. 19, n. 119, p. 534-559, out. 2017/jan. 2018.

VERBICARO, Dennis. **Consumo e cidadania**: identificando os espaços políticos de atuação qualificada do consumidor. Rio de Janeiro: Lumen Juris, 2017.

VERBICARO, Dennis. **Consumo e cidadania**: identificando os espaços políticos de atuação qualificada do consumidor. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

VERBICARO, Dennis. O controle da publicidade ilícita: uma análise reflexiva dos sistemas consumeristas brasileiro e espanhol. **Revista Cesumar Ciências Humanas e Sociais Aplicadas**, Maringá, PR, v. 21, n. 2, p. 261-285, jul./dez. 2016.

VERBICARO, Dennis; ALCÂNTARA, Ana Beatriz Quintas Santiago de. A (in)eficácia do dever informacional nas relações de consumo: como superar a desconfiança recíproca entre consumidores e fornecedores no ambiente pré-contratual. **Revista Eletrônica Direito e Sociedade**, Canoas, v. 5, n. 1, p. 9-26, maio 2017a.

VERBICARO, Dennis; ALCÂNTARA, Ana Beatriz Quintas Santiago de. A percepção do sexismo face à cultura do consumo e a hipervulnerabilidade da mulher no âmbito do assédio discriminatório de gênero. **Revista Pensamento Jurídico**, São Paulo, v. 11, n. 1, p. 172-192, jan./jun. 2017b.

VERBICARO, Dennis; ATAÍDE, Camille da Silva Azevedo. O crédito como objeto de tensão qualificada na relação de consumo e a necessidade de prevenção ao superendividamento. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, v. esp., n. 36, p. 74-89, 2017.

VERBICARO, Dennis; CAÇAPIETRA, Ricardo dos Santos. A economia comportamental no desenho de políticas públicas de consumo através dos nudges. **Revista de Direito do Consumidor**, São Paulo, v. 30, n. 133, p. 385-411, jan./fev. 2021.

VERBICARO, Dennis; COSTA, Emanuelle Dias. A atuação qualificada das associações de defesa do consumidor como expressão de uma democracia deliberativa: mapeamento da atuação judicial e extrajudicial no âmbito do Estado do Pará. **Revista Eletrônica Direito e Sociedade,** Canoas, v. 6, n. 2, p. 69-86, set. 2018.

VERBICARO, Dennis; FREIRE, Gabriela Ohana Rocha. O combate ao dumping social no mercado de consumo através do exercício qualificado da liberdade de escolha do consumidor. **Revista de Direito, Globalização e Responsabilidade nas Relações de Consumo**, Porto Alegre, v. 4, n. 2, p. 1-18, jul./dez. 2018.

VERBICARO, Dennis; MARTINS, Ana Paula Pereira. A contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 116, p. 369-391, mar./abr. 2018.

VERBICARO, Dennis; OHANA, Gabriela; VIEIRA, Janaina do Nascimento. A mediação online como ferramenta de empoderamento do consumidor ou estratégia utilitarista para redução das demandas de consumo? **Revista Científica Disruptiva**, [*s.l.*], v. 2, n. 2, p. 40-62, jul./dez. 2020.

VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camille. Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológico do assédio de consumo. *In*: VERBICARO, Dennis; ATAÍDE, Camille; ACIOLI, Carlos (coord.). **Provocações contemporâneas no direito do consumidor**. Rio de Janeiro: Lumen Juris, 2018. p. 167-204.

VERBICARO, Dennis; VERBICARO, Loiane da Ponte Souza Prado. A indústria cultural e o caráter fictício da individualidade na definição do conceito de consumidor-comunidade global. **Revista Jurídica Cesumar**, Maringá, PR, v. 17, n. 1, p. 107-131, jan./abr. 2017.

VERBICARO, Dennis; VIEIRA, Janaina do Nascimento. A hipervulnerabilidade do turista e a responsabilidade das plataformas digitais: uma análise a partir da perspectiva da economia colaborativa. **Revista de Direito do Consumidor**, São Paulo, v. 29, n. 127, p. 305-330, 2020a.

VERBICARO, Dennis; VIEIRA, Janaina do Nascimento. A prova estatística na tutela coletiva de consumo. **Revista *Thesis Juris***, São Paulo, v. 9, n. 2, p. 361-379, jul./dez. 2020b.

VERBICARO, Dennis; VIEIRA, Janaina do Nascimento. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**, São Paulo, v. 30, n. 134, p. 195-226, mar./abr. 2021.

VERBICARO, Dennis. VIEIRA, Janaina. A objetificação sexista da mulher nas relações de consumo a luz da teoria feminista de Mackinnon. **Revista da Faculdade de Direito da UFPR**, Curitiba, [2021b], No prelo.

VIAL, Sofhia Martini. A sociedade da (des)informação e os contratos de comércio eletrônico: do Código Civil às atualizações do Código de Defesa do Consumidor, um necessário diálogo entre fontes. **Revista de Direito do Consumidor**, São Paulo, v. 22, n. 88, p. 229-257, jul./ago. 2013.

VIEIRA, Janaina do Nascimento. **O superendividado como a expressão do *Homo Sacer*.** 2019. Trabalho apresentado no 38º Congresso Nacional do Conpedi, Belém, 2019.

VIEIRA, Janaina; OHANA, Gabriela. Do consumo analógico à aceleração do consumo digital: o paradoxo entre consumidor vidro e consumidor identitário no pós-covid 19. *In:* VERBICARO, Dennis; VERBICARO, Loiane Prado (coord.). **Tensões de uma sociedade em crise**. Rio de Janeiro: Lumen Juris, 2020. p. 449-458.

WALDMAN, Ari Ezra. Designing Without Privacy. **Houston Law Review**, [*s.l.*], v. 55, n. 659, p. 659-727, 2018.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Cambridge, MA, v. 4, n. 5, p. 193-220, Dec. 1890.

WESTIN, Alan. **Privacy and Freedom.** New York: Athenum, 1967.

WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **Revista do Advogado**, Rio de Janeiro, ano 39, n. 144, p. 126-133, nov. 2019.

XAVIER, José Tadeu; RIEMENSCHNEIDER, Patrícia. A vulnerabilidade agravada do consumidor nas situações relacionadas à maternidade. **Revista de Direito do Consumidor**, São Paulo, v. 28, n. 121, p. 277-322, jan./fev. 2019.

ZAMPIER, Bruno. **Bens digitais**: cybercultura, redes sociais, e-mails, músicas, livros, milhas aéreas, moedas virtuais. São Paulo: Editora Foco, 2017.

ZANATTA, Rafael A. F. A tutela coletiva na proteção de dados pessoais. **Revista do Advogado**, Rio de Janeiro, ano 39, n. 144, p. 201-208, nov. 2019.

ZANATTA, Rafael A. F.; SOUZA, Michel R. O. A tutela coletiva em proteção de dados pessoais: tendências e desafios. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). **Direito e Internet IV**: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019. p. 381-418.

ZANCHET, Marília. A nova força obrigatória dos contratos e o princípio da confiança no ordenamento jurídico brasileiro: uma análise comparativa entre o CDC e o CC de 2002. **Revista de Direito do Consumidor**, São Paulo, n. 58, p. 116-142, abr./jun. 2006.

ZAK, Paul. **A molécula da moralidade**: as surpreendentes descobertas sobre a substância que desperta o melhor em nós. Rio de Janeiro: Elsevier, 2012.

ZAVASCKI, Teori Albino. **Processo coletivo**: tutela de direitos coletivos e tutela coletiva de direitos. 2. ed. São Paulo: Revista dos Tribunais, 2007.

ZETTER, Kim. Anonymized Phone Location Data Not So Anonymous, Researchers Find. **Wired**, 27 mar. 2013. Disponível em: https://www.wired.com/2013/03/anonymous-phone-location-data/. Acesso em: 18 abr. 2020.

ZITTRAIN, Jonathan. A History of Online Gatekeeping. **Harvard Journal of Law and Technology**, Cambridge, MA, v. 19, n. 2, p. 253-298, Spring 2006.

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

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: A luta por um futuro humano na nova fronteira de poder. Tradução George Schlesinger. Rio de Janeiro: Intrínseca, 2020.