

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ
ESCOLA DE DIREITO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD**

RAFAEL ALMEIDA OLIVEIRA REIS

**DIÁLOGOS ENTRE SOCIEDADE DE RISCO E SOCIEDADE
INFORMACIONAL: HIPERCONNECTIVIDADE E A REGULAÇÃO DA
PROTEÇÃO DE DADOS PESSOAIS NO BRASIL**

CURITIBA

2023

RAFAEL ALMEIDA OLIVEIRA REIS

**DIÁLOGOS ENTRE SOCIEDADE DE RISCO E SOCIEDADE
INFORMACIONAL: HIPERCONNECTIVIDADE E A REGULAÇÃO DA
PROTEÇÃO DE DADOS PESSOAIS NO BRASIL**

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de Mestre em Direito.

Orientadora: Prof.^a Dr.^a Cinthia Obladen de Almendra Freitas.

CURITIBA

2023

Dados da Catalogação na Publicação
Pontifícia Universidade Católica do Paraná
Sistema Integrado de Bibliotecas – SIBI/PUCPR
Biblioteca Central
Sônia Maria Magalhães da Silva – CRB 9/1191

R375d 2023	Reis, Rafael Almeida Oliveira Diálogos entre sociedade de risco e sociedade informacional : hiperconectividade e a regulação da proteção de dados pessoais no Brasil / Rafael Almeida Oliveira Reis ; orientadora: Cinthia Obladen de Almendra Freitas. – 2023 153 f. : 30 cm Dissertação (mestrado) – Pontifícia Universidade Católica do Paraná, Curitiba, 2023 Bibliografia: f. 141-153 1. Sociedade da informação. 2. Proteção de dados. 3. Brasil. Lei geral de proteção de dados pessoais (2018). 4. Inovações tecnológicas. 5. Direito. I. Freitas, Cinthia Obladen de Almendra. II. Pontifícia Universidade Católica do Paraná. Programa de Pós-Graduação em Direito. III. Título. Doris 3. ed. – 340
---------------	--

TERMO DE APROVAÇÃO

RAFAEL ALMEIDA OLIVEIRA REIS

DIÁLOGOS ENTRE SOCIEDADE DE RISCO E SOCIEDADE INFORMACIONAL: HIPERCONECTIVIDADE E A REGULAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Dissertação apresentada ao Programa de Pós-Graduação em Direito, na área de concentração de Direito Socioambiental e Sustentabilidade e na linha de pesquisa em Estado, Sociedades, Povos e Meio Ambiente, da Escola de Direito da Pontifícia Universidade Católica do Paraná, como requisito parcial à obtenção do título de Mestre em Direito.

COMISSÃO EXAMINADORA

Prof.^a Dr.^a Cinthia Obladen de Almendra Freitas.
Orientador PPGD – PUCPR

Prof.^a Dr.^a Heline Sivini Ferreira
Membro PPGD – PUCPR

Prof. Dr. Marcos Wachowicz
Membro externo – UFPR

Professora Dra. Claudia Maria Barbosa
Membro PPGD – PUCPR – Suplente

Curitiba, 14 de abril de 2023.

“É um meio-termo entre dois vícios, um por excesso e outro por falta, pois nos vícios ou há falta ou há excesso daquilo que é conveniente no que concerne às ações e às paixões, ao passo que a virtude encontra e escolhe o meio-termo.”

Aristóteles

AGRADECIMENTOS

À minha esposa, Camilla, pelo constante apoio e compreensão na árdua caminhada para a realização deste trabalho. Minha eterna fonte de inspiração por seu foco e determinação sem precedentes.

Aos meus pais, Sinfrônio e Simone, por terem me proporcionado as condições necessárias para que houvesse mais vitórias do que derrotas em minha trajetória.

Aos meus sogros, Marcos e Limi, por terem participado de todas as etapas deste trabalho e por me acolherem como um filho.

À minha irmã, Patricia, por sua ternura e por suprir a minha ausência nos negócios da família durante a realização do mestrado.

À minha família, por ser uma constante fonte de amor e carinho.

Ao meu grande amigo, Lucas Bossoni Saikali, por ter me incentivado à vida acadêmica e pela tão gentil ajuda na revisão do trabalho.

Aos amigos que a vida me deu, pelas conversas, conselhos e momentos proporcionados.

Aos queridos colegas da Becker Direito Empresarial, pelo suporte e incentivo.

Aos integrantes da Comissão de Inovação e Gestão da OAB/PR, por proporcionarem o ambiente necessário de discussões para que eu pudesse ter contato com temas inovadores no Direito e pessoas brilhantes.

À minha orientadora, Prof.^a Dr.^a Cinthia Obladen de Almendra Freitas, por sua incondicional paixão pela pesquisa e por tornar a minha caminhada acadêmica mais leve. Por seu desvelo nas orientações, sua paciência e notável sabedoria.

Aos profissionais e colegas do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná, que, sempre com muita atenção, ajudaram-me com meus pedidos e dúvidas em relação ao programa.

À Coordenação de Aperfeiçoamento de Pessoal (CAPES), pelo meu vínculo ao Programa de Excelência Acadêmica (PROEX), o que permitiu o custeio de meus estudos, e que espero retribuir, com este trabalho, à pesquisa jurídica no Brasil.

RESUMO

Adotando as teorias da Sociedade em Rede de Manuel Castells e a Sociedade de Risco de Ulrich Beck como marcos teóricos, a pesquisa cria diálogos entre as duas teorias, especialmente em relação à produção sistemática de riscos à privacidade criados pelo emprego das Tecnologias da Informação e Comunicação (TICs) e como esses riscos podem assumir características catastróficas para toda a humanidade, demandando a avaliação de alternativas regulatórias para a sua mitigação. Aplicando o método dedutivo, partiu-se da constatação de que a sociedade moderna vivencia um expressivo processo de transformação capitaneado pelas TICs. O advento da Internet lançou as bases de novos avanços que culminaram nos marcos tecnológicos do Big Data e da Inteligência Artificial, consumando uma nova realidade hiperconectada marcada por riscos à privacidade e democracia. Paralelamente, a criação sistemática de riscos à privacidade na Sociedade Informacional passa a expressar uma modalidade diferenciada da Sociedade de Risco, revelando os contornos digitais de sua caracterização. Nesse cenário, examinou-se o regime de proteção de dados pessoais no Brasil, identificando a relação dos riscos com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), bem como de que forma as organizações podem mitigar as ameaças criadas pelo uso das TICs por meio de ferramentas de governança e *compliance*. Constatou-se que o Direito não é, por si só, um instrumento efetivo para regular o comportamento das diversas organizações que realizam tratamento de dados pessoais, o que levou à análise do *Privacy by Design*, da regulação por arquitetura e o papel da Autoridade Nacional de Proteção de Dados (ANPD) para uma concreta tutela da privacidade no Brasil. Por fim, concluiu-se que o modelo regulatório de arquitetura pode ser o mais adequado para orientar o desenvolvimento da proteção de dados pessoais no Brasil, devendo sua aplicação ser incentivada pela ANPD.

Palavras-chave: Sociedades. Sociedade Informacional. Sociedade de Risco. Novas Tecnologias. Regulação. Privacidade. Proteção de Dados Pessoais.

ABSTRACT

Adopting the theories of the Network Society by Manuel Castells and the Society of Risk by Ulrich Beck as theoretical frameworks, Adopting the theories of Manuel Castells' Network Society and Ulrich Beck's Risk Society as theoretical frameworks, the research creates dialogues between the two theories, especially concerning the systematic production of privacy risks created by the use of Information and Communication Technologies (ICTs) and how these risks can take on catastrophic characteristics for all of humanity, demanding the evaluation of regulatory alternatives for their mitigation. Applying the deductive method, it started from the observation that modern society experiences a significant process of transformation led by ICTs. The advent of the Internet laid the foundations for new advances that culminated in the technological milestones of Big Data and Artificial Intelligence, consummating a new hyperconnected reality marked by risks to privacy and democracy. Simultaneously, the systematic creation of privacy risks in the Informational Society begins to express a differentiated modality of the Risk Society, revealing the digital contours of its characterization. In this scenario, the personal data protection regime in Brazil was examined, identifying the relationship of risks with the General Data Protection Law (Law No. 13,709/2018), as well as how organizations can mitigate the threats created by the use of ICTs through governance and compliance tools. It was found that the Law is not, by itself, an effective instrument to regulate the behavior of various organizations that process personal data, which led to the analysis of Privacy by Design, regulation by architecture, and the role of the National Data Protection Authority (ANPD) for concrete privacy protection in Brazil. In conclusion, it was determined that the architectural regulatory model may be the most suitable for guiding the development of personal data protection in Brazil, and its application should be encouraged by ANPD.

Keywords: Societies. Information Society. Risk Society. New technologies. Regulation. Privacy. Personal Data Protection.

LISTA DE TABELAS

Tabela 1 - Riscos ligados ao tratamento de dados pessoais	122
---	-----

TABELA DE ABREVIATURAS E SIGLAS

ANATEL	Agência Nacional de Telecomunicações
ANEEL	Agência Nacional de Energia Elétrica
ANPD	Autoridade Nacional de Proteção de Dados
ARPA	<i>Advanced Research Projects Agency</i>
ARPANET	<i>Advanced Research Projects Agency Network</i>
CC	Código Civil
CDC	Código de Defesa do Consumidor
CERN	<i>European Organization for Nuclear Research</i>
COBIT	<i>Control Objectives for Information and related Technology</i>
CRFB	Constituição da República Federativa do Brasil
DCA	<i>Defense Communication Agency</i>
DNT	<i>Do Not Track</i>
HTML	<i>Hyper Text Markup Language</i>
HTTP	<i>Hyper Text Transfer Protocol</i>
IA	Inteligência Artificial
IANA/ICANN	Autoridade para Atribuição de Números na Internet
IOT	<i>Internet of Things</i>
IP	<i>Internet Protocol</i>
IPTO	<i>Information Processing Techniques Office</i>
ISACA	<i>Information Systems Audit and Control Association</i>
ISO	<i>International Organization for Standardization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
ITSM	<i>for IT Service Management</i>
LAI	Lei de Acesso à Informação
LCP	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
MILNET	<i>Military Network</i>
MIT	<i>Massachusetts Institute of Technology</i>
NWG	<i>Network Working Group</i>
PdD	<i>Privacy by Design</i>
PET's	<i>Privacy Enhancing Technologies</i>
RFC'S	<i>Request For Comments</i>
RGPD	Regulamento Geral de Proteção de Dados
RIPD	Relatório de Impacto à Proteção de Dados
TCP	<i>Transmission Control Protocol</i>
TI	Tecnologia da Informação
TIC'S	Tecnologias da Informação e Comunicação
TISA	<i>Trade In Services Agreement</i>

TPP	<i>Trans-Pacific Partnership</i>
TTIP	<i>Transatlantic Trade and Investment Partnership</i>
URL	<i>Uniform Resource Locator</i>
W3C	<i>World Wide Web Consortium</i>
WWW	<i>World Wide Web</i>

SUMÁRIO

INTRODUÇÃO	12
1. ERA DA INFORMAÇÃO E SOCIEDADE DO RISCO: DUAS FACES DE UMA NOVA MODERNIDADE	18
1.1. O CAPITALISMO E A REVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO	19
1.2. CARACTERÍSTICAS DA REVOLUÇÃO TECNOLÓGICA E O ADVENTO DA SOCIEDADE INFORMACIONAL	29
1.3. O PAPEL DO ESTADO NO DESENVOLVIMENTO DAS TICS E O PARADIGMA DA TECNOLOGIA DA INFORMAÇÃO	33
1.4. UMA MODERNIDADE REFLEXIVA: A TEORIA DA SOCIEDADE DE RISCO.....	37
1.5. A CONFIGURAÇÃO DA SOCIEDADE DE RISCO E A CONSTRUÇÃO INSTITUCIONAL DO RISCO	48
1.6. UMA NOVA MODERNIDADE A PARTIR DE ULRICH BECK	51
2. HIPERCONNECTIVIDADE NA SOCIEDADE INFORMACIONAL E OS RISCOS À PRIVACIDADE	53
2.1. O ADVENTO DA INTERNET E DA CONECTIVIDADE	57
2.2. O <i>BIG DATA</i> COMO NOVO MARCO TECNOLÓGICO: HIPERCONNECTIVIDADE E TRATAMENTO DE DADOS	65
2.3. CONSEQUÊNCIAS DA HIPERCONNECTIVIDADE PARA A CRIAÇÃO DE RISCOS DA SOCIEDADE INFORMACIONAL.....	72
2.4. PRIVACIDADE E TRATAMENTO DE DADOS PESSOAIS NA SOCIEDADE HIPERCONNECTADA.....	81
2.5. CONTORNOS DA DIMENSÃO DIGITAL DA SOCIEDADE DE RISCO.....	86
3. REGIME DA PROTEÇÃO DE DADOS NO BRASIL, FERRAMENTAS DE MITIGAÇÃO DE RISCO E A REGULAÇÃO POR ARQUITETURA	95
3.1. DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS	97
3.2. REGIME DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL.....	102
3.3. A RELAÇÃO DOS RISCOS COM A LGPD	110

3.4. MITIGAÇÃO DE RISCOS NA SOCIEDADE INFORMACIONAL: FERRAMENTAS DE GESTÃO DE RISCO E <i>COMPLIANCE</i>	116
3.5. O <i>PRIVACY BY DESIGN</i> E A REGULAÇÃO POR ARQUITETURA COMO RESPOSTA AOS RISCOS CRIADOS PELA SOCIEDADE INFORMACIONAL	124
3.6. O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PARA A TUTELA DA PRIVACIDADE	130
CONCLUSÃO	136
REFERÊNCIAS	141

INTRODUÇÃO

Se na sociedade industrial clássica ainda era possível prever quais seriam os impactos do uso das tecnologias para a evolução da sociedade, hoje pairam dúvidas sobre o modo como o ser humano se relaciona com elas em uma sociedade hiperconectada. Se são muitos os benefícios oriundos de uma Sociedade Informacional, natural que os seus aspectos negativos sejam colocados em segundo plano, em vistas a acelerar o processo de desenvolvimento econômico e de inovação tecnológica.

Hoje, entre os principais impactos causados por esses avanços e pela ampla circulação de informações por meio das Tecnologias de Informação e Comunicação (TIC's), estão aqueles que impactam negativamente os direitos da personalidade, especialmente a privacidade. Se no passado o tratamento de dados pessoais era de interesse praticamente exclusivo do Estado para identificar características de sua população, produzindo informações imprescindíveis para a definição de políticas públicas e investimentos, hoje, todavia, o uso de dados pessoais move a atividade econômica mais próspera do planeta¹, sendo a “matéria-prima” de uma infinidade de organizações privadas altamente lucrativas.

Assim, já não basta proteger o homem contra os desmandos do Estado. Aliás, igualmente não basta proteger o homem contra as agressões das grandes corporações que dominam as plataformas digitais e redes sociais. Em uma sociedade pouco atenta aos efeitos não antecipados pelas novas tecnologias, por vezes é necessário evitar que o próprio homem renuncie aos direitos que consagram a dignidade humana como fundamento da liberdade e valor central da ordem jurídica.

A relevância do tema não pode ser maior. Os impactos das TICs em uma sociedade hiperconectada tem o potencial de reduzir a pessoa à condição de mero objeto de tratamento de dados por incontáveis organizações em todo o

¹ Entre as quinze maiores empresas do mundo em valor de mercado, oito tem como principal ativo o tratamento de dados pessoais em escala global. Cf.: The 100 largest companies in the world by market capitalization in 2022. Economy & Politics, Economy. In: **Statista Research Department**, 2022. Disponível em: <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/>. Acesso em: 02 fev. 2023.

mundo, estabelecendo fluxos de dados transfronteiriços com finalidades pouco transparentes, bem como de forma praticamente imperceptível, invisível.

A Declaração Universal dos Direitos Humanos de 1948 afirma que o “reconhecimento da dignidade inerente a todos os membros da família humana e de seus direitos iguais e inalienáveis é o fundamento da liberdade, da justiça e da paz no mundo”.² A dignidade humana é sacramentada, portanto, como “fundamento da liberdade”, conceito que influenciou diversas Constituições mundo afora, inclusive a brasileira, que, em seu art. 1º, inc. III, estabeleceu como fundamento do Estado Democrático de Direito a “a dignidade da pessoa humana.”³

Proteger a condição humana nos seus mais legítimos aspectos e manifestações torna-se uma missão primordial do Direito, especialmente em uma sociedade hiperconectada. A tarefa, porém, não é simples.

O desenvolvimento de novas TICs, especialmente após a revolução da Internet e, mais recentemente, do *Big Data*, provocou verdadeiras mudanças de paradigmas tecnológicos em vários campos do conhecimento com o potencial de, a partir do emprego de computadores, sistemas de comunicação, *Machine Learning* (Aprendizagem de Máquina), análise preditiva, entre outros, transformar o modo como a humanidade se desenvolve, trabalha, se relaciona em sociedade, enfim, como vive.

Nesse contexto, o próprio modo de produção capitalista se desloca. Com a substituição dos bens materiais para os serviços culturais, a base da produção da sociedade se torna imaterial e fluida, potencializando ainda mais esse processo irrefreável de mudanças definitivas no corpo da sociedade, que passa a se organizar em redes de informação e conhecimento.

Os benefícios desse processo de modernização são de fato incontáveis e indiscutíveis. Novas tecnologias melhoram não só a vida das pessoas em geral, mas também aumentam a eficiência e produtividade das indústrias, permitem a comunicação em colaboração em escala global e geram crescimento

² UNITED NATIONS. **Universal Declaration of Human Rights**. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 02 fev. 2023.

³ BRASIL. **Constituição da República Federativa do Brasil, 1988**. Brasília-DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 mar. 2022.

econômico, aumentando a riqueza e a prosperidade nos países mais desenvolvidos tecnologicamente.

Todas essas mudanças, todavia, não vêm sem consequências. Se para produzir bens essenciais ao ser humano a indústria tradicional produz resíduos que prejudicam o meio ambiente, o desenvolvimento das TICs pode atingir um “bem” tão ou mais valioso ao ser humano, qual seja a sua personalidade traduzida em direitos fundamentais.

Essas consequências, todavia, ainda são pouco compreendidas, pelo menos para a sociedade em geral. O avassalador desenvolvimento econômico provocado pelas gigantes da tecnologia (*Big Techs*) faz com que haja uma corrida pela próxima revolução tecnológica, sem que ocorra sequer uma compreensão dos riscos provocados pelas anteriores.

São diversos os estudos que relacionam o emprego das TICs com a criação de riscos ao ser humano, tanto em seu plano individual ou coletivo. A Inteligência Artificial, por exemplo, recentemente ganhou um novo marco com o desenvolvimento de modelos de processamento de linguagem natural que são capazes de responder, por meio de cálculos probabilísticos e milhões de páginas da Internet mapeadas, qualquer pergunta inserida por um ser humano.⁴ Sem dúvida uma ferramenta fantástica, mas também capaz de reforçar ou perpetuar preconceitos e discriminações existentes na sociedade.

Em seu espectro coletivo, as TICs já mostraram alguns dos riscos que são capazes de criar. O escândalo *Cambridge Analytica*, por exemplo, envolveu o uso indevido de dados pessoais de milhões de usuários do Facebook para construir modelos psicológicos e influenciar a opinião dos eleitores durante a campanha presidencial dos Estados Unidos em 2016 e no referendo do *Brexit*⁵ no mesmo ano. Há cada vez mais evidências de como a tecnologia baseada no tratamento de dados pessoais pode ser utilizada para manipular e modular o

⁴ Os modelos de processamento de linguagem natural são capazes de processar imagens e textos e gerar respostas, também chamadas de *outputs*, com grande capacidade de interação com o ser humano. Tais modelos são um importante marco na evolução de sistemas baseados em princípios de Inteligência Artificial pois apresentam um potencial de serem utilizados para uma vasta gama de aplicações como sistemas de diálogos com seres humanos (*chats*), sumarização de textos, traduções, entre outros. Cf.: OpenAI. GPT-4 Technical Report. 2023. Disponível em: <https://doi.org/10.48550/arXiv.2303.08774>.

⁵ Brexit se refere ao processo de saída do Reino Unido da União Europeia que teve início em 2017 e foi concluído em 2020.

comportamento humano com as mais diversas finalidades, desde a já citada manipulação política até para fins puramente comerciais e comportamentais.

É essencial, portanto, compreender de que forma a sociedade, suas organizações e indivíduos, lidam com os riscos concebidos a partir da evolução tecnológica propiciada no último século pelo surgimento da Sociedade Informacional e as TICs.

Diante disso, a pesquisa para essa dissertação de Mestrado surgiu da preocupação com o modo passivo pelo qual o tema tem sido encarado pela sociedade, ignorando – por vezes de forma propositada – os riscos provocados pelo seu próprio desenvolvimento. Buscou-se, para isso, proposições teóricas que pudessem explicar esse fenômeno.

As reflexões propostas pautam-se, nesse sentido, em 02 (dois) marcos teóricos: a teoria da Sociedade Informacional de Manuel Castells e a teoria da Sociedade de Risco proposta pelo sociólogo alemão Ulrich Beck, que argumenta que a sociedade moderna está em um estágio de sua evolução em que não se pode mais controlar os riscos criados pela modernidade.

Embora esta teoria social tenha revolucionado a visão dos riscos ecológicos criados pela sociedade industrial moderna, parte-se da premissa de que o trabalho do sociólogo alemão suscita discussões sobre novos riscos globais e abstratos que geram graves consequências ao meio ambiente. Em uma visão amplificada dessa teoria, buscam-se respostas para uma dimensão digital da Sociedade de Risco, abrangendo o contexto dos paradigmas tecnológicos provocados pelo advento da Sociedade Informacional e da hiperconectividade para a criação de riscos catastróficos e imensuráveis.

Nesse sentido, a hipótese inicial do presente trabalho compreende a existência de uma dimensão digital da Sociedade de Risco, com características e riscos próprios, especialmente em relação à privacidade, que passam a gerar consequências catastróficas em todo o mundo, para a atual e futuras gerações, demandando uma nova abordagem regulatória para que essas consequências possam ser, pelo menos em parte, controladas. Busca-se, nesse sentido, uma resposta para conciliar o desejável desenvolvimento tecnológico e social e a redução dos riscos dessas tecnologias para a humanidade.

O objetivo geral da pesquisa foi compreender de que modo a Sociedade Informacional expressa uma dimensão digital da Sociedade de Risco, conforme

a proposta pelo sociólogo alemão Ulrich Beck, englobando os riscos criados a partir do emprego das Tecnologias da Informação e Comunicação, especialmente em relação aos riscos que impactam a privacidade, bem como quais são os potenciais formas de mitigação desses riscos. Como objetivos específicos, tem-se: (i) Examinar os pressupostos da Sociedade em Rede, de Manuel Castells e da Sociedade de Risco proposto pelo sociólogo Ulrich Beck; (ii) Identificar diálogos entre as teorias da Sociedade em Rede e da Sociedade de Risco; (iii) Compreender a composição dos riscos dessas sociedades, especialmente os ligados a utilização das tecnologias da informação e comunicação (TICs); (iv) Relacionar as consequências da hiperconectividade provocada por tecnologias como a Internet e o *Big Data* com as características da Sociedade de Risco; (v) Identificar os elementos que caracterizam a dimensão digital da Sociedade de Risco; (vi) Examinar a evolução da privacidade e o regime de proteção de dados pessoais no Brasil; e (vii) Compreender quais as ferramentas disponíveis para a mitigação dos riscos na Sociedade Informacional.

Com esse propósito, em termos de metodologia científica, utilizou-se o método hipotético-dedutivo e o procedimento monográfico de revisão bibliográfica, na medida em que, a partir de considerações lógicas interligadas, busca-se entender como a Sociedade de Risco pode ser também compreendida em sua esfera digital, na qual a Sociedade Informacional e o emprego das TICs criam riscos tão ou mais relevantes do que aqueles inicialmente previstos pelo teórico alemão, e de que forma eles podem ser mitigados a partir de ferramentas de gestão de risco e regulação.

O desenvolvimento metodológico deste projeto compreende 03 (três) momentos principais. No Capítulo 1, parte-se da obra do sociólogo espanhol Manuel Castells como referencial teórico, abordando os pressupostos e características da Sociedade Informacional, especialmente em relação ao papel da revolução tecnológica por meio do emprego das TICs e as transformações daí decorrentes no modelo capitalista de produção. Em um segundo momento, adentra-se na análise da teoria da Sociedade de Risco proposta por Ulrich Beck, que teoriza sobre o modo como o processo de modernização da sociedade industrial clássica culmina em uma Sociedade de Risco, caracterizada pela

produção sistemática de riscos catastróficos que passam a ser ameaças globais que escapam à percepção do homem.

No Capítulo 2, parte-se das tecnologias desenvolvidas no contexto da Sociedade Informacional que culminam na criação de riscos e ameaças globais à humanidade. São analisadas as tecnologias que, com o apoio da Internet e do *Big Data*, aumentam a interconexão e interdependência entre indivíduos, organizações e governos por meio de objetos físicos, sensores, algoritmos, entre outros, que, além de inquestionáveis benefícios, acabam por criar riscos à personalidade humana, notadamente ao direito fundamental à privacidade. Nesse sentido, propõe-se uma relação entre a criação de riscos à privacidade no ambiente da Sociedade Informacional com as características da Sociedade de Risco teorizada por Ulrich Beck, estabelecendo os seus contornos para além das consequências ambientais da atividade humana.

Por fim, no Capítulo 3, embrenhou-se na evolução do conceito da privacidade até o seu hodierno entendimento como direito à proteção de dados pessoais, bem como na análise do regime de proteção de dados pessoais no Brasil e o modo com que seu maior expoente, a Lei Geral de Proteção de Dados, relaciona-se com os riscos criados pelas organizações que tratam dados pessoais. Finalmente, são exploradas algumas ferramentas aptas a mitigar os riscos da Sociedade Informacional, especialmente no contexto da atuação da Autoridade Nacional de Proteção de Dados e o seu papel de regulação do mercado.

A pesquisa se enquadra na área de concentração de “Direito Socioambiental e Sustentabilidade”, uma vez que os impactos da utilização das TICs podem provocar ameaças globais ao ser humano, afetando, em seu plano individual, o livre desenvolvimento da personalidade, e, em espectro coletivo, o próprio Estado Democrático de Direito. Em relação à linha de pesquisa “Estado, Sociedades, Povos e Meio Ambiente”, o trabalho relaciona a Sociedade Informacional e a Sociedade de Risco, procurando estabelecer ligações entre as duas teorias e algumas propostas para um maior equilíbrio entre o desenvolvimento econômico e a sustentabilidade.

1. SOCIEDADE INFORMACIONAL E SOCIEDADE DE RISCO: DIÁLOGOS DA MODERNIDADE

Para compreender o processo de transformação social ocasionado pelas Tecnologias da Informação e Comunicação (TICs) nas últimas décadas, é necessário compreender de que modo essas mudanças alteraram a lógica de funcionamento das sociedades, inclusive em relação ao seu modo de produção dominante no Ocidente – o capitalismo. Assim como a energia elétrica transformou a sociedade industrial na segunda metade do século XVIII, mais recentemente o surgimento das TICs revolucionou o modo como a humanidade se relaciona socialmente, a ponto de haver uma ruptura de paradigmas sem precedentes.⁶

Essas transformações sociais, ocorrem especialmente a partir da passagem da sociedade industrial clássica do século XIX, para dar origem a uma nova modernidade. São vários os autores que trabalham esse período histórico de intensa transformação das bases da sociedade. São objetivos de estudo neste capítulo, particularmente duas teorias sociológicas que visam estudar esse período histórico. A primeira delas, proposta pelo sociólogo espanhol Manuel Castells, defende que a sociedade industrial clássica deu lugar a um novo modo de desenvolvimento. Se antes o desenvolvimento da sociedade estava centrado na indústria, no curso da história surge um modo de desenvolvimento centrado na informação.⁷ Daí, a expressão cunhada pelo autor que denomina esse novo estágio da humanidade, organizada em torno de uma “sociedade informacional”.

A segunda teoria abordada nesse capítulo, é a proposta pelo sociólogo alemão Ulrich Beck, que caracteriza esse processo de modernização, ou seja, a transição da sociedade industrial clássica - denominada pelo autor como “primeira modernidade”, para uma outra configuração social que acaba por

⁶ Manuel Castells define essa ruptura como o Paradigma da Tecnologia da Informação, vide tópico 1.3. Cf.: CASTELLS, Manuel. **A Sociedade em Rede**. Tradução Roneide Venancio Majer, 22. ed. São Paulo: Paz e Terra, 2020.p. 87.

⁷ CASTELLS, *op. cit.*, p. 77.

dissolver os contornos da sociedade industrial⁸. A esse estágio, o autor denomina de “segunda modernidade”, ou, “Sociedade de Risco”⁹.

Para que seja possível estudar as transformações e os impactos dessas mudanças, especialmente no campo do desenvolvimento das TICs e, por consequência, as suas repercussões na criação de riscos aos indivíduos e em toda a coletividade, foram examinados, como marcos teóricos, os pressupostos de ambas as teorias sociológicas, para, no Capítulo 2 (dois), estabelecer relações entre o uso de novas tecnologias e a criação sistemática de riscos à sociedade, um dos elementos constituintes da Sociedade de Risco proposta por Ulrich Beck.

1.1. O CAPITALISMO E A REVOLUÇÃO DA TECNOLOGIA DA INFORMAÇÃO

Manuel Castells, em sua teoria sociológica sobre a Sociedade em Rede, descreve o modo histórico com que as sociedades se organizam. Sua obra é, em conjunto com os estudos sobre a Sociedade de Risco de Ulrich Beck, a base teórica do presente trabalho, sendo ela fundamental para a compreensão dos marcos históricos que culminaram no advento da Sociedade Informacional¹⁰ e na definição de suas características próprias. O autor espanhol propõe, ao se debruçar sobre as transformações sociais decorrentes desse processo de evolução tecnológica, a criação de novo paradigma social e tecnológico.

⁸ BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011. p. 13.

⁹ De forma objetiva, a Sociedade de Rico pode ser definida como: i) uma sociedade catastrófica, em que o estado de emergência ameaça tornar-se o estado normal; ii) O risco relativiza a posição de classe, ou seja, atinge pobres e ricos, seja em relação aos riscos ecológicos, mas também em relação aos ricos derivados de uma sociedade altamente conectada; iii) A produção de riscos não contradiz a lógica de valoração do capital, muito pelo contrário, há um aproveitamento econômico dos riscos; iv) O risco ressalta o papel da consciência e exige da sociologia contribuição para uma teoria do surgimento e divulgação da consciência do risco. Vide tópico 1.5.

¹⁰ Ao estudar a sociedade industrial, seus paradigmas e traços sociotécnicos, Manuel Castells então propõe que, da mesma forma que se fala em uma sociedade industrial, também se poderia falar da existência de uma nova sociedade informacional, marcada por uma série de características fundamentais comuns em seus sistemas sociotécnicos. Cf.: CASTELLS, *op. cit.*, p. 77.

Para ele, as sociedades têm como premissas as “relações historicamente determinadas de produção, experiência e poder”.¹¹ Essas relações e construções sociológicas são utilizadas para caracterizar as sociedades ao longo de 02 (dois) eixos: modos de produção e de desenvolvimento.¹²

Embora não seja objetivo desse trabalho realizar um detalhado histórico do modo de produção capitalista, é necessário compreender a sua origem para que seja possível analisar como as TICs modificaram o modo em que a sociedade se comporta e tolera os riscos criados por ela mesma, bem como de que forma o próprio capitalismo sofreu profundas alterações a partir do desenvolvimento das TICs.

Segundo Castells, modos de produção podem ser caracterizados pela relação entre a mão de obra humana e a matéria no processo de trabalho utilizando os meios de produção, que por sua vez são definidos como os instrumentos utilizados para agir sobre a matéria. Nesse contexto, a tecnologia¹³, em seu sentido estrito, pode ser considerada como o resultado da relação entre “a mão de obra e a matéria no processo de trabalho”¹⁴. Essa relação só é possível com o uso dos meios de produção para agir sobre a matéria, que por sua vez podem ser baseados em energia, informação ou conhecimento. A tecnologia de uma sociedade é, portanto, o resultado da relação entre esses elementos, apresentando variações conforme o tempo e a sociedade em que ela se aplica e desenvolve.¹⁵ Essa interação que determina a tecnologia de uma sociedade define o seu modo de desenvolvimento, que está posteriormente analisado.

¹¹ Nesse sentido, as relações de produção são caracterizadas pela ação do homem sobre a natureza para fins de apropriação própria, seja para seu consumo ou para acumulação de um excedente que poderá ser utilizado como investimento conforme objetivos socialmente determinados. Essa produção é organizada em relações de classes que definem a divisão e os empregos do produto em relação ao consumo e ao investimento, a depender da posição do sujeito no processo produtivo. A experiência, por sua vez, tem relação com a ação dos sujeitos humanos sobre si mesmos em seus ambientes sociais e naturais. Sua principal característica é a busca incessante do ser humano pela satisfação de suas necessidades e desejos. Já o poder é a relação entre os humanos que, com base na produção e na experiência, impõe a vontade de alguns sobre os outros pelo emprego potencial ou real de violência física ou simbólica. Esse poder tem como base o Estado e o seu monopólio institucionalizado do uso da violência. Cf.: CASTELLS, *op. cit.*, p. 72.

¹² *ibid.*, p. 72.

¹³ Tecnologia pode ser conceituado como "o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível". (*ibid.*, p. 54).

¹⁴ *ibid.*, p. 73.

¹⁵ CASTELLS, *op. cit.*, p. 72.

O resultado dessas relações de produção – ou seja, o seu produto – pode ser utilizado pelo homem para seu consumo próprio ou, caso o resultado da sua produção exceda as necessidades básicas para a subsistência do homem, para a criação de um excedente. As estruturas sociais caracterizadas pelas relações de produção, experiência e poder, conforme analisado anteriormente, interagem com esses processos produtivos para determinar as regras de apropriação, distribuição e uso do excedente.

Para Castells, “essas regras constituem modos de produção, e esses modos definem as relações sociais de produção, determinando a existência de classes sociais, constituídas como tais mediante sua prática histórica”¹⁶, ou seja, o princípio estrutural de apropriação e controle do excedente de uma sociedade é o que caracteriza o seu modo de produção.

No século XX, houve 02 (dois) modos predominantes de produção: (i) capitalismo e (ii) estatismo. Este último, por não ser objeto de estudo do presente trabalho, pode ser resumido como um modo de produção que confere um controle externo à esfera econômica do excedente produzido pela sociedade. Ou seja, toda a produção da sociedade e distribuição do excedente fica sob as mãos dos detentores do poder estatal.¹⁷

No capitalismo, por sua vez, há uma separação fundamental entre os produtores dos bens da sociedade dos seus meios de produção. O trabalho, nesse sentido, é transformado em *commodity*, e há posse privada dos meios de produção com base no controle do capital. O objetivo máximo do capitalismo é, dessa forma, a maximização dos lucros por meio do aumento do excedente apropriado pelo controle privado dos meios de produção.¹⁸

Segundo a perspectiva de Adam Smith, o crescimento econômico de uma sociedade capitalista só é possível quando uma parcela da população possui um suprimento de matérias-primas ou de bens manufaturados maior do que suas

¹⁶ *ibid.*, p. 73.

¹⁷ *ibid.*, p. 73.

¹⁸ *ibid.*, p. 73.

necessidades imediatas, possibilitando, assim, a criação do excedente.¹⁹ O capitalista, portanto, é motivado por um interesse pessoal.²⁰

Karl Marx, em sua obra-prima sobre o capital, descreve o surgimento do capitalismo como um “processo histórico que dissocia o trabalhador dos meios de produção”. Esse processo nasce na estrutura econômica da sociedade feudal, com a expropriação dos meios de produção do trabalhador.²¹

A revolução definitiva que culmina no modelo capitalista de produção ocorre no último terço do século XV e nas primeiras décadas do século XVI, com a dissolução das vassalagens feudais, lançando ao mercado de trabalho uma massa de indivíduos que passam a vender a sua força de trabalho em troca de dinheiro. Com isso, o até então predominante modelo da nobreza sucumbe, dando lugar ao dinheiro como “poder dos poderes”.²²

Em sua gênese, o capitalismo é centrado no comércio entre as pessoas, viabilizado pela criação do excedente de bens manufaturados. O desenvolvimento de novas tecnologias²³ culmina na primeira revolução industrial do século XVIII, induzindo novos comportamentos nas bases materiais da economia, sociedade e cultura. O cerne dessa transformação se dá pelas

¹⁹ Esse excedente oferece a oportunidade de comércio entre as pessoas. Haverá, nesse contexto, a especialização das pessoas na produção de um certo produto enquanto houver demanda por esse produto que supra a necessidade do produtor das suas outras necessidades. Inicia-se, nesse contexto, uma divisão do trabalho que irá se desenvolver até que alguns trabalhadores só estejam produzindo uma pequena parte de um produto manufaturado. Essa especialização aumenta a produtividade e dá início à produção em massa. Cf.: MORRISON, Wayne. **Filosofia do Direito: dos gregos ao pós-modernismo**. São Paulo: Martins Fontes, 2006. p. 214).

²⁰ O "capitalista é involuntariamente levado a trabalhar para satisfazer essas necessidades sociais, pois, ainda que busque o próprio lucro, contribui para o bem-estar geral "uma mão invisível leva-o a lutar por um objetivo que não estava entre suas intenções". O bem-estar geral - avaliado como o aumento dos bens de consumo e, desse modo, como a satisfação pelo seu uso - será mais bem atendido ao se permitir que cada pessoa persiga seus próprios interesses. Cf.: MORRISON, *op. cit.*, p. 215.

²¹ Segundo Karl Marx, a acumulação primitiva pode ser definida um “processo histórico que dissocia o trabalhador dos meios de produção”. Esse processo nasce na estrutura econômica da sociedade feudal, com a libertação da servidão e da coerção corporativa. “Mas os que se emanciparam só se tornaram vendedores de si mesmos depois que lhes roubaram todos os seus meios de produção e os privaram de todas as garantias que as velhas instituições feudais asseguravam à sua existência”. Nessa toada, contribui para esse processo a expropriação do produtor rural e do camponês, que são privados de suas terras – sendo essa a base de todo o processo. Cf.: MARX, Karl. **O capital: crítica da economia política**. Livro primeiro. São Paulo: Abril Cultural, 1984. p. 830.

²² MARX, *op. cit.*, p. 343.

²³ Essas inovações tecnológicas transformaram o trabalho manual, até então predominante, em trabalho em série, possibilitado pela substituição da força humana pela máquina. Cf.: LIMA, E. C. DE; OLIVEIRA NETO, C. R. DE. Revolução Industrial: considerações sobre o pioneirismo industrial inglês. **Revista Espaço Acadêmico**, v. 17, n. 194, p. 102-113, 6 jul. 2017.

modificações nas relações entre a mão-de-obra e a matéria nos processos produtivos.

Um modo de produção, portanto, determina a forma de apropriação e uso do excedente. O nível desse excedente é determinado pela produtividade do processo produtivo, ou seja:

[...] pelo índice do valor de cada unidade de produção em relação ao valor de cada unidade de insumos. Os próprios níveis de produtividade dependem da relação entre a mão de obra e a matéria, como uma função do uso dos meios de produção pela aplicação de energia e conhecimentos. Esse processo é caracterizado pelas relações técnicas de produção, que definem modos de desenvolvimento.²⁴

O modo de desenvolvimento de uma sociedade, como dito por Castells, envolve as relações técnicas de produção, ou seja, é o modo pelo qual os trabalhadores atuam sobre a matéria para gerar determinado produto. Quanto maior a produtividade desse modelo, maior será o nível e qualidade do excedente. A tecnologia, nesse sentido, é o que vai definir e dar forma a essa relação, determinando qual o nível de produtividade da sociedade.²⁵

A sociedade agrária, por exemplo – anterior à sociedade industrial, tinha como fonte de incremento de excedente os aumentos quantitativos de mão de obra e dos recursos naturais no processo produtivo. Já na sociedade industrial, as fontes de produtividade residiam nas novas fontes de energia e no uso de máquinas que aumentaram a produtividade com a criação dos métodos produtivos e das fábricas.²⁶

Na sociedade pós-industrial, denominada por Manuel Castells como Sociedade Informacional, a fonte de produtividade encontra-se na tecnologia de geração de conhecimento, nos métodos de processamento de dados e nas tecnologias de comunicação de símbolos:

Conhecimento e informação são elementos cruciais de todos os modos de desenvolvimento, visto que todo processo produtivo se baseia em algum tipo de conhecimento e processamento de informação. O verdadeiro diferencial do modo de desenvolvimento informacional é a

²⁴ CASTELLS, *op. cit.*, p. 74.

²⁵ *ibid.*, p. 74.

²⁶ Houve pelo menos duas revoluções industriais. Uma no século XVIII, caracterizada por novas tecnologias como a máquina a vapor, a fiadeira e, de forma geral, da substituição das ferramentas manuais pelas máquinas. A segunda ocorre aproximadamente 100 anos depois, destacada pelo desenvolvimento da eletricidade, motor a combustão, produtos químicos, fundição do aço e do início das tecnologias da comunicação com o telégrafo e o telefone. (*ibid.*, p. 91).

ação do conhecimento sobre os próprios conhecimentos como principal fonte de produtividade. O processamento da informação é focalizado na melhoria da tecnologia para melhorar a geração de conhecimentos e o processamento da informação.²⁷

Para que seja possível compreender o significado e a dimensão dessa mudança de paradigma, é necessário definir os significados de dados, informação e conhecimento. Segundo Davenport, dados são o resultado de “simples observações sobre o estado do mundo”²⁸, ou seja, da quantificação de fatos brutos, que pode ser feita tanto por pessoas ou por algum tipo de tecnologia aplicada. Informação, por sua vez, exige um processo de análise para que os dados sejam dotados de “relevância e propósito”²⁹ para um determinado fim. Para que a informação gere um significado, é necessário um consenso e, impreterivelmente, uma mediação humana. Por fim, conhecimento é informação mais interpretação, reflexão, contexto, síntese, entre outros. Trata-se da “informação mais valiosa da mente humana”³⁰. Dito isso, se há, conforme Castells, ação do conhecimento sobre o conhecimento por meio de tecnologias de processamento da informação, menciona-se então um modelo de desenvolvimento que utiliza as TICs para interpretar dados em volumes cada vez maiores, transferindo informações a um custo cada vez menor, interpretando-as de forma cada vez mais eficiente, em um ciclo contínuo e retroalimentado. Se o conhecimento é a informação mais valiosa da mente humana, as TICs passam a ser o seu carro forte mais poderoso.

Esse processo de ação do conhecimento sobre o conhecimento, característico da Sociedade Informacional, é um fator histórico decisivo, segundo Castells, para o surgimento de um novo paradigma tecnológico baseado na Tecnologia da Informação (TI). Tais relações técnicas de produção no modo de desenvolvimento informacional se difundem em todo o conjunto de relações e estruturas sociais. Uma vez que ela se baseia em conhecimento e informação, há uma íntima ligação entre as forças produtivas, o espírito e a matéria, gerando novas formas históricas de interação, controle e transformação social.³¹

²⁷ *ibid.*, p. 74.

²⁸ DAVENPORT, T. H. **Ecologia da informação**: porque só a tecnologia não basta par o sucesso na era da informação. Tradução B. S. Abrão. São Paulo: Futura, 1988. p.18.

²⁹ DAVENPORT, *op. cit.*, p. 18.

³⁰ *ibid.*, p. 19.

³¹ CASTELLS, *op. cit.*, p. 75.

Essas transformações ocorrem especialmente após o final da 2ª. Guerra Mundial, e se intensifica na década de 70 com o processo de reestruturação capitalista que culmina no capitalismo informacional³². A obra de Manuel Castells estuda de que forma o surgimento de uma nova condição social - a sociedade em rede - ocorre. Essa estrutura é manifestada sob várias formas, mas tem como principal associação o surgimento de um novo modo de desenvolvimento, o informacionalismo, que foi historicamente moldado pela decadência da sociedade industrial e pela reestruturação do modo capitalista de produção no final do século XX.³³

Uma outra proposta de formulação da Sociedade Informacional é a idealizada por Yoneji Masuda, autor do Plano Japonês para uma Sociedade Informacional na década de 1970.³⁴ Embora utópica, o referido autor desenvolve conceitos ligados ao uso da tecnologia dos computadores que substituem e amplificam o trabalho intelectual dos homens, permitindo a produção em massa de conhecimento, passando a ser o principal ativo econômico das indústrias e sociedades.³⁵ Isso, ao que parece, se revelou verdadeiro, especialmente nos últimos 20 anos com o desenvolvimento e massificação da Internet.

Se a Sociedade Informacional, como visto, é uma evolução ou um estágio pós sociedade industrial, é necessário compreender o contexto em que ocorre esse processo de transformação que acaba por modificar não só a sociedade moderna, mas, também, o modo de funcionamento do próprio capitalismo.

No passado, foram os privilégios estamentais e a igreja que passaram por um processo de desencantamento, a realidade social do século XXI é marcada pela imensurável influência digital na vida das pessoas. Vive-se em um mundo que se tornou digital³⁶, caracterizado por sua excepcional capacidade de conectar os campos tecnológicos com uma linguagem digital comum que gera, armazena, processa e transmite informações.³⁷ A revolução da Tecnologia da

³² O termo faz referência ao processo de reestruturação capitalista que ocorreu a partir dos anos 1980 e gerou um novo sistema econômico e tecnológico. (CASTELLS, *op. cit.*, p. 75.)

³³ *ibid.*, p. 72.

³⁴ MASUDA, Yoneji. **A Sociedade Informacional como sociedade pós-industrial**. Tradução Kival Chaves Weber e Angela Melim. Rio de Janeiro: Ed. Rio, 1982.

³⁵ WERTHEIN, J. A Sociedade Informacional e seus desafios. **Ciência da Informação**, [S. l.], v. 29, n. 2, 2000, p. 74. Disponível em: <https://revista.ibict.br/ciinf/article/view/889>. Acesso em: 21 out. 2022.

³⁶ NEGROPONTE, N. **A Vida Digital**. São Paulo: Companhia das Letras, 1995. p. 88.

³⁷ CASTELLS, *op. cit.*, p. 88.

Informação é diferente pois ela se retroalimenta, ou seja, aplicam-se os conhecimentos gerados no próprio desenvolvimento da tecnologia elaborada, acelerando seu processo de transformação³⁸ e conectando o mundo por meio da tecnologia da informação.³⁹

Hoje, é o entendimento científico e tecnológico da sociedade industrial clássica que passa por esse desencantamento e desconstrução. Há uma modificação fundamental no papel da família, do trabalho e das relações entre homens e mulheres que vivem na modernidade.⁴⁰ Esse é um evento histórico da mesma magnitude da primeira revolução industrial do século XVIII, que provocou um padrão de ruptura nos fundamentos materiais da economia, sociedade e cultura. Diferentemente de qualquer outra revolução, a essência da transformação que se vive na revolução atual refere-se essencialmente às TICs.⁴¹

A Segunda Guerra Mundial e os anos que a sucederam são caracterizados pelas principais descobertas tecnológicas do século XX. Alan Turing⁴² cria sua máquina revolucionária e dá início a era da computação. Nas décadas seguintes, várias descobertas em microeletrônica culminam na invenção do microprocessador e de outras tecnologias inovadoras.⁴³ Na sequência, com a redução de custo de processamento por meio de *chips* cada vez menores e mais baratos, o desenvolvimento das telecomunicações e a integração dos computadores em rede transformam as TICs, abrindo as portas para a revolução tecnológica no final do século XX.⁴⁴

Essa intensificação na evolução de novas tecnologias da informação ocorrida a partir da década de 70 gera uma aceleração do seu desenvolvimento. Cada grande avanço em campos tecnológicos específicos amplia os efeitos das

³⁸ *ibid.*, p. 114.

³⁹ *ibid.*, p. 88.

⁴⁰ BECK, 2015, *op. cit.*, p. 13.

⁴¹ CASTELLS, *op. cit.*, p. 88.

⁴² Alan Mathison Turing nasceu em Paddington, Londres, em 23 de junho de 1912. Dedicou seus estudos às formas e especificidades para o reconhecimento das linguagens formais: classificação, propriedades, características e inter-relacionamentos. Formulou o conceito de algoritmo e criou a chamada “máquina de Turing”, um dispositivo teórico que estabelecia os princípios do computador, por meio de um conceito de máquina universal. Cf.: PETRAGLIA, I. C.; PALMISANO, A.; ROSINI, A. M. Alan Turing: cientista complexo e transdisciplinar. **Debates em Educação**, [S. l.], v. 12, n. 28, p. 596–609, 2020. Disponível em: <https://www.seer.ufal.br/index.php/debateseducacao/article/view/9769>. Acesso em: 2 out. 2022.

⁴³ CASTELLS, *op. cit.*, p. 96.

⁴⁴ *ibid.*, p. 109.

tecnologias conexas. Não obstante, um outro fator histórico característico dessa revolução tecnológica foi responsável pela sua arrasadora aceleração:

[...] o fator histórico mais decisivo para a aceleração, encaminhamento e formação do paradigma da tecnologia da informação e para a indução de suas conseqüentes formas sociais foi/é o processo de reestruturação capitalista, empreendido desde os anos 1980, de modo que o novo sistema econômico e tecnológico pode ser adequadamente caracterizado como capitalismo informacional.⁴⁵

Nessa circunstância, é na década de 80 que o capitalismo passa por um profundo movimento de reestruturação organizacional. As TICs exercem um papel fundamental nesse processo e, em um movimento inverso, também são profundamente moldadas pelo seu papel desempenhado nesse contexto. Esse ambiente turbulento conduz um movimento empresarial de desregulamentação e liberalização que foi decisivo para o crescimento da telecomunicação, especialmente nos Estados Unidos da América.⁴⁶

O advento da sociedade informacional está, portanto, intimamente ligado à uma “expansão e ao rejuvenescimento”⁴⁷ do capitalismo, assim como a revolução industrial foi o marco de constituição desse modo de produção. Ulrich Beck, ao retratar esse processo de transformação, afirmou que:

[...] assim como no século XIX a modernização dissolveu a esclerosada sociedade agrária estamental e, ao depurá-la, extraiu a imagem estrutural da sociedade industrial, hoje a modernização dissolve os contornos da sociedade industrial e, na continuidade da modernidade, surge uma outra configuração social.⁴⁸

Portanto, e conforme expõe Manuel Castells em sua obra, o surgimento da Sociedade em Rede não deve ser compreendido sem levar em consideração “duas tendências relativamente autônomas: 1) o desenvolvimento de novas

⁴⁵ *ibid.*, p. 75.

⁴⁶ *ibid.*, p. 115.

⁴⁷ O modelo de crescimento capitalista que trouxe estabilidade para as 3 décadas posteriores à segunda guerra mundial alcançou sua limitação na década de 1970. Com os aumentos do petróleo em 74 e 79, governos e empresas passaram a buscar um processo de reestruturação num método pragmático de tentativa e erro, que continuou durante a década de 90, quando houve um maior esforço a favor da desregulamentação (inclusive no Brasil, com uma série de privatizações, etc.) Uma série de reformas buscaram 4 objetivos: 1) aprofundar a lógica capitalista em busca de lucro nas relações de capital/trabalho; 2) aumentar a produtividade do trabalho e do capital; 3) globalizar a produção, circulação e mercados; 4) direcionar apoio estatal para ganhos de produtividade e competitividade das economias nacionais em detrimento da proteção social e das normas de interesse público. Cf.: CASTELLS, *op. cit.*, p. 76.

⁴⁸ BECK, 2015, *op. cit.*, p. 12.

tecnologias da informação e; 2) a tentativa da antiga sociedade de reaparelhar-se com o uso do poder da tecnologia.”⁴⁹

Esse novo paradigma tecnológico conta com algumas premissas básicas. Embora essas tecnologias sejam baseadas principalmente em conhecimentos já existentes na sociedade industrial, elas representaram um grande avanço qualitativo na disseminação maciça da tecnologia em aplicações militares, comerciais e civis, especialmente por conta da sua acessibilidade cada vez maior, com custo marginal cada vez menor e com maior qualidade.

No entanto, a grande revolução que amplifica os efeitos das TICs e altera de forma irreversível a sociedade pós-industrial é a criação da *Internet*, tecnologia baseada em troca de pacotes que criou o conceito das redes descentralizadas⁵⁰ e provoca a convergência definitiva de praticamente todas as tecnologias da comunicação.⁵¹ A *Internet* foi e é o meio tecnológico mais revolucionário da era da informação, e passa a determinar a lógica de funcionamento de redes, permeando todas os tipos de atividades humanas, conectando contextos, locais e qualquer coisa que possa ser conectada eletronicamente.⁵²

Evidente que, mesmo com o surgimento da Sociedade Informacional e do capitalismo informacional, isso não implica no desaparecimento do industrialismo (nem mesmo do modo de desenvolvimento agrário), mas eles são profundamente afetados pelo novo paradigma da Sociedade Informacional:

Continuamos a produzir trigo e arroz, aço e automóveis, mas o elemento básico de formação do valor, o fator principal de produção, é constituído por um conjunto de atividades intangíveis que podem ser generalizadas sem custos adicionais significativos.⁵³

Nesse sentido, o eixo dominante da estruturação social passa a ser o acesso à informação e ao controle do conhecimento, bem como a acumulação industrial passou a dominar o conjunto das relações sociais de produção na segunda metade do século XIX e XX. Não obstante, a indústria e a agricultura expandem a sua capacidade produtiva com a incorporação dos avanços

⁴⁹ CASTELLS, *op. cit.*, p. 115.

⁵⁰ Vide tópico 2.1. Cf.: CASTELLS, *op. cit.*, p. 101.

⁵¹ *ibid.*, p. 100.

⁵² CASTELLS, *op. cit.*, p. 107.

⁵³ DOWBOR, Ladislau. **O capitalismo se desloca**: novas arquiteturas sociais. São Paulo: Edições Sesc-SP, 2020. p. 45.

intangíveis que passam a dominar as transformações em praticamente todas as áreas do conhecimento.⁵⁴

Ladislau Dowbor, em sua obra sobre as mudanças sofridas pelo capitalismo nas últimas décadas, desenvolve a ideia de que as tecnologias provocam mais do que uma transformação no modo capitalista de produção, elas acarretam um deslocamento da sua base material da produção física para o imaterial.⁵⁵ Tais transformações são tão profundas quanto as da Revolução Industrial, mas nesse novo contexto “a nova máquina da sociedade é o conhecimento, tornando-se a nova base da economia.”⁵⁶ Assim, as TICs são, para esta revolução, o que as novas fontes de energia foram para as revoluções anteriores.⁵⁷

Apresentam-se adiante essas transformações e o “deslocamento” do capitalismo provocando grandes efeitos na sociedade. Estas, ao assumirem uma característica de fluxo globalizado, provocam consequências incontrolláveis nas esferas individuais e coletivas. Elas são, por definição, a expressão do mercado capitalista informacional, agora radicalizado pelas TICs e livre dos controles dos Estados.⁵⁸

1.2. CARACTERÍSTICAS DA REVOLUÇÃO TECNOLÓGICA E O ADVENTO DA SOCIEDADE INFORMACIONAL

A revolução capitaneada pela TICs tem como principal característica a sua retroalimentação - conhecimento agindo sobre o conhecimento, e a aplicação dessa informação na geração de conhecimento, processamento, comunicação e dispositivos num ciclo de convergência e inovação cumulativa de tecnologias em microeletrônica, computação, desenvolvimento de softwares, telecomunicações, radiodifusão, etc.⁵⁹ Se antes a revolução industrial importou o acoplamento de máquinas a novas fontes energéticas, na revolução das

⁵⁴ DOWBOR, *op. cit.*, p. 38.

⁵⁵ "O principal fator de produção (no caso informacional) não é escasso, e isso explica inclusive por que tantas corporações buscam gerar artificialmente escassez para poder cobrar o acesso, como se verifica com a propriedade intelectual. Cf.: DOWBOR, *op. cit.*, p. 29.

⁵⁶ *ibid.*, p. 31.

⁵⁷ Castells descreve essa evolução como sendo os desenvolvimentos do motor a vapor à eletricidade, dos combustíveis fósseis à energia nuclear. Cf.: CASTELLS, *op. cit.*, p. 88.

⁵⁸ BECK, 2015, *op. cit.*, p. 29.

⁵⁹ CASTELLS, *op. cit.*, p. 88.

tecnologias da informação “o homem programa a operação das máquinas”.⁶⁰ Isso ocorre, mais recentemente, pelo desenvolvimento de técnicas para tratamento e dados, informações e conhecimento como a Mineração de Dados, entendido como o “pré-processamento, extração e exploração de grandes quantidades de dados visando estabelecer padrões consistentes”⁶¹, e o *Big Data*, expressão dada a um conjunto de dados com características próprias, tais como grande volume e variedade, bem como altas velocidades de transferência.⁶²

Há, também, nessa revolução, uma nítida característica de substituição dos bens materiais pelos serviços culturais ou o conhecimento, caracterizados como atividades informativas que incorporam um conjunto de recursos consumidos na produção, no processamento e na distribuição dos bens e serviços informativos como nova base da sociedade pós-industrial. Nesse sentido, Marcos Wachowicz afirma que “a revolução da Tecnologia da Informação representou para a economia uma autêntica segunda Revolução Industrial, expressa pelo surgimento de um quarto setor informacional”.⁶³

Sendo o conhecimento um bem imaterial, ele é fluido e pode ser apropriado sem custos marginais. Nesse contexto, alteram-se os riscos e perigos da sociedade, exigindo uma maior atenção para a proteção e defesa da personalidade, da cultura e da propriedade intelectual em um mundo cada vez mais virtualizado e globalizado.⁶⁴ Não por acaso, as maiores e mais prósperas organizações do mundo não são mais as grandes fábricas, mas quem controla as plataformas digitais, aplicativos, patentes, *copyrights*. Esta última, em um movimento de adaptação às mudanças da sociedade informacional, ao invés de criminalizar o compartilhamento de arquivos na *Internet*, passou a utilizar conceitos de trabalho cooperativo em plataformas digitais e o barateamento dos produtos e serviços por meio da negociação de dados pessoais de seus

⁶⁰ DOWBOR, *op. cit.*, p. 29.

⁶¹ BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de Dados e Privacidade: Do direito às novas tecnologias na Sociedade Informacional.** Rio de Janeiro: Lúmen, 2018. p. 191.

⁶² Esse conceito é mais detalhadamente explorado no segundo capítulo. Cf.: BOFF; FORTES; FREITAS, 2018, *op. cit.*, p. 214.

⁶³ WACHOWICZ, M. Os impactos das novas tecnologias da informação. **Revista do Direito**, n. 28, p. 54-89, 25 jul. 2007.

⁶⁴ TOURAINE, 1994 *apud* CASTELLS, *op. cit.*, p. 78.

usuários.⁶⁵ Há, nesse sentido, um deslocamento para uma economia baseada em dados e conhecimento, altamente tecnológica, cujo produto normalmente se reveste de uma roupagem digital como os *softwares*, as plataformas de economia compartilhada e sistemas baseados em *Big Data* e ferramentas dotadas de inteligência artificial.⁶⁶

Nesse sentido, as TICs são, a partir da revolução e mudanças, estudadas no tópico anterior, o principal fator de produção da sociedade moderna. Para Ladislau Dowbor, “constata-se um deslocamento teórico fundamental para a compreensão dos novos processos: não se trata de propriedade dos meios de produção, se sim do controle dos sistemas.”⁶⁷ Cuida-se, portanto, de uma nova economia, totalmente orientada por dados, informação e conhecimento. Diferente de outras revoluções, ela se difundiu com grande velocidade em menos de duas décadas, influenciada por um período histórico de reestruturação do capitalismo. A tecnologia foi, nesse sentido, essencial para que o capitalismo informacional se desenvolvesse:

Ela originou-se e difundiu-se, não por acaso, em um período histórico da reestruturação global do capitalismo, para o qual foi uma ferramenta básica. Portanto, a nova sociedade emergente desse processo de transformação é capitalista e também informacional, embora apresente variação histórica considerável nos diferentes países, conforme sua história, cultura, instituições e relação específica com o capitalismo global e a tecnologia informacional.⁶⁸

Essa intensa e rápida difusão se dá por uma lógica própria dessa revolução: "a aplicação imediata no próprio desenvolvimento da tecnologia gerada, conectando o mundo através da tecnologia da informação".⁶⁹ E conforme as TICs foram desenvolvidas, estas passaram por 03 (três) momentos distintos de evolução nas últimas décadas: (i) a automação de tarefas, (ii) as experiências de usos e (iii) a reconfiguração das aplicações. Nos dois primeiros momentos, o desenvolvimento da inovação tecnológica baseou-se em aprender usando. No último, os usuários aprenderam a tecnologia fazendo, resultando,

⁶⁵ SILVEIRA, S. Amadeu da. A noção de modulação e os sistemas algorítmicos. **PAULUS**: Revista de Comunicação da FAPCOM, [S. l.], v. 3, n. 6, 2019. p. 33. Disponível em: <https://fapcom.edu.br/revista/index.php/revista-paulus/article/view/111>. Acesso em: 22 nov. 2022.

⁶⁶ DOWBOR, *op. cit.*, p. 35.

⁶⁷ *ibid.*, p. 35.

⁶⁸ CASTELLS, *op. cit.*, p. 71.

⁶⁹ *ibid.*, p. 90.

segundo Castells, na reconfiguração permanente das redes e num ciclo contínuo de descoberta de novas aplicações.⁷⁰

Outra característica, embora indireta, dessa revolução tecnológica são suas implicações nas relações de trabalho, que passam a ser flexibilizadas em relação a sua jornada e local, uma vez que tudo pode ser conectado. Essa característica, segundo Ulrich Beck, dilui as fronteiras entre o trabalho e o ócio:

A microeletrônica permite reconectar setores, empresas e consumidores a despeito dos setores produtivos. Dessa forma, porém, as atuais premissas jurídicas e sociais do sistema empregatício são "modernizadas até desaparecerem": o desemprego em massa é integrado ao sistema empregatício sob formas de novas de "subemprego plural" - com todos os riscos e oportunidades implicados.⁷¹

Por fim, essa revolução tem o potencial, se é que não se pode dizer que ele já foi atingido, a partir da utilização de computadores, sistemas de comunicação, técnicas de mineração de dados, utilização de grandes bancos de dados *Big Data*, com processamento e velocidades cada vez maiores e com custos menores, de transformar o modo como a humanidade se desenvolve, trabalha, produz, enfim, como ela vive. Não obstante, esse emaranhado de tecnologias da informação e comunicação cria uma rede global de informação e conhecimento potencialmente ubíqua e, junto com todos os potenciais de inovação benéficos à sociedade, cria-se uma rede pervasiva que, por vezes, cria riscos sistemáticos aos seus usuários, especialmente em relação à privacidade.⁷²

Essa revolução tecnológica culmina, finalmente, no advento denominado por Manuel Castells como Sociedade Informacional, sistema sociotécnico com características próprias que o diferem da sociedade industrial clássica.

Seu surgimento pode ser entendido como a interação entre o desenvolvimento de novas Tecnologias da Informação e Comunicação e a tentativa de reaparelhamento do capitalismo com o uso do poder da tecnologia, para, assim, "servir a tecnologia do poder".⁷³

⁷⁰ CASTELLS, *op. cit.*, p. 89.

⁷¹ BECK, 2015, *op. cit.*, p. 17.

⁷² CASTELLS, *op. cit.*, p. 89.

⁷³ *ibid.*, p. 115.

Assim, a sociedade informacional surge como uma tendência histórica que modifica de forma irreversível as lógicas dos processos produtivos, da experiência, poder e cultura. A vida passa a ser organizada em torno de redes, que passam a constituir a morfologia social de nossa sociedade, com estruturas flexíveis que podem se expandir e integrar novas tecnologias de forma ilimitada:

Com base nessas tecnologias, os cientistas da computação preveem a possibilidade de ambientes de processamento nos quais bilhões de microscópicos aparelhos de processamento de dados se espalharão por toda a parte "como pigmentos de tinta de paredes". Se isso acontecer mesmo, então as redes de computadores serão, materialmente falando, a trama da nossa vida.⁷⁴

Deste modo, a lógica das redes, conforme idealizado por Castells, passa a ser o principal instrumento da economia capitalista voltada para a inovação e globalização, criando interações e desconstruindo padrões sociais, num ciclo de desconstrução e reconstrução contínua. Ela é flexível e adaptável, e seu principal expoente – a *Internet* – passou a dominar a vida e conectar todas as pessoas, atividades, contextos e locais que possam ser conectados eletronicamente.⁷⁵

Embora nas últimas décadas esse processo de desenvolvimento de novas tecnologias tenha como principais patrocinadores as organizações privadas, no início dessa revolução o Estado teve um papel fundamental, se não decisivo, para que fossem criados os ambientes propícios para a construção de novas tecnologias – também chamados de ambientes de inovação.⁷⁶ Sem isso, provavelmente não haveria Sociedade Informacional, bem como as mudanças de paradigma provocados pela Tecnologia da Informação.

1.3. O PAPEL DO ESTADO NO DESENVOLVIMENTO DAS TICS E O PARADIGMA DA TECNOLOGIA DA INFORMAÇÃO

A primeira revolução em Tecnologia de Informação e Comunicação concentrou-se nos EUA, especialmente na região do Vale do Silício (Califórnia), a partir da década de 1970. Segundo Castells, esse processo foi mais um resultado de indução tecnológica do que determinação social, especialmente

⁷⁴ CASTELLS, *op. cit.*, p. 108.

⁷⁵ *ibid.*, p. 107.

⁷⁶ *ibid.*, p. 119.

devido às características contextuais dessa região, que o autor descreve como “ambientes de inovação”:

[...] o desenvolvimento da revolução da tecnologia da informação contribuiu para a formação dos meios de inovação em que as descobertas e as aplicações interagem e eram testadas em um repetido processo de tentativa e erro: aprendia-se fazendo. Esses ambientes exigiam (e no início do século XXI ainda exigem, apesar da atuação online) a concentração espacial de centros de pesquisa, instituições de educação superior, empresas de tecnologia avançada e uma rede auxiliar de fornecedores, provendo bens e serviços e redes de empresas com capital de risco para financiar novos empreendimentos. Em segundo lugar, uma vez que um meio esteja consolidado, como o Vale do Silício na década de 1970, ele tende a gerar sua própria dinâmica e a atrair conhecimentos, investimentos e talentos de todas as partes do mundo.⁷⁷

Nesse sentido, o desenvolvimento da revolução da tecnologia da informação contribuiu para a formação dos meios de inovação.⁷⁸ Não obstante, o autor atribui à atuação do Estado, se não como um fator determinante, enquanto um agente decisivo para o desenvolvimento e aceleração dos progressos ligados às TICs. Isso ocorre pois ele pode, especialmente por meio de sua intervenção na economia, organizar as forças sociais dominantes para incentivar esse processo de modernização tecnológica e, assim, “mudar o destino de economias, do poder militar e do bem-estar social em poucos anos”.⁷⁹

Assim, foi o Estado e não o empreendedor de “inovações em garagem” quem iniciou a revolução da tecnologia da informação, tanto nos Estados Unidos quanto no mundo.⁸⁰ Todavia, desde a década de 70 esse processo de inovação tem sido conduzido pelo mercado de forma acelerada. Nesse contexto, o processo de inovação se intensifica em velocidade e difusão, conforme pessoas talentosas, movidas por um propósito ou ambição, fazem pesquisas de nicho em busca de um “oceano azul”.⁸¹

⁷⁷ CASTELLS, *op. cit.*, p. 119.

⁷⁸ O desenvolvimento da revolução da tecnologia da informação contribuiu para a formação dos meios de inovação em que as descobertas e as aplicações interagem e eram testadas em um repetido processo de tentativa e erro: aprendia-se fazendo. Cf.: CASTELLS, *op. cit.*, p. 119.

⁷⁹ *ibid.*, p. 66.

⁸⁰ MAZZUCATO, Mariana. **O estado empreendedor**: desmascarando o mito do setor público x setor privado. São Paulo: Portfolio-Penguin, 2014.

⁸¹ Segundo Castells “[...] é mediante essa interface entre os programas de macropesquisa e grandes mercados desenvolvidos pelos governos, por um lado, e a inovação descentralizada estimulada por uma cultura de criatividade tecnológica e por modelos de sucessos pessoais rápidos, por outro, que as novas tecnologias da informação prosperam. No processo, essas tecnologias agruparam-se em torno de redes de empresas, organizações e instituições para formar um novo paradigma sociotécnico.” (*ibid.*, p. 123).

Esse processo também conduziu um processo de desregulamentação e liberalização liderada pelo movimento empresarial na década de 80, sendo um fator decisivo para a reorganização e o crescimento das tecnologias de telecomunicações e, conforme visto em capítulos anteriores, do desenvolvimento (ou renascimento) do próprio capitalismo.⁸²

Sem esse conjunto específico de fatores, tanto em relação à indução do Estado para criar o ambiente necessário para o desenvolvimento de novas tecnologias, quanto pela atuação de um liberalismo econômico vinculados a processos de desregulamentação para incentivar o mercado a investir em novas tecnologias, o paradigma da Tecnologia da Informação dificilmente seria viabilizado.

É interessante notar que esses fatores ajudam a compreender as duas faces desse progresso tecnológico que, embora induzido pelo Estado, passa a se desenvolver em um ambiente desregulado. O resultado desses ingredientes são produtos e serviços que modificaram e melhoraram a vida das pessoas, mas que, ao não se submeterem a um entendimento público dos seus impactos com transparência e uma dose de regulação, provocaram a criação de riscos de difícil solução.

Nesse sentido, a obra de Manuel Castells busca esclarecer a dinâmica econômica e social da nova era da informação, bem como estabelecer as bases desse novo paradigma sociotécnico. O seu surgimento está muito ligado às descobertas e à uma dinâmica específica da era da informação: à convergência tecnológica e seus efeitos sinérgicos.

A partir desse paradigma, o ciclo de realimentação entre a criação de uma nova tecnologia, seu uso e desenvolvimento se torna muito mais rápido, tornando criadores e usuários a mesma coisa. Os processos sociais e culturais são rapidamente transformados em bens e serviços, uma vez que a mente humana é a força direta de produção.⁸³

⁸² *ibid.*, p. 115.

⁸³ Nesse sentido, o microprocessador possibilitou o microcomputador e os avanços em telecomunicações permitiu a conexão dos computadores. As inúmeras aplicações dessas tecnologias permitiram uma ampliação dos potenciais de novas tecnologias de fabricação de chips e semicondutores. Assim, códigos foram desenvolvidos pelo mercado crescente de softwares e aplicativos. Por fim, houve uma explosão da conexão de dispositivos com a expansão da rede em uma teia mundial voltada para o usuário. Cf.: CASTELLS, *op. cit.*, pp. 89-114.

Todo esse contexto tecnológico determina as características do paradigma da tecnologia da informação, conforme proposto por Castells. i) A informação é sua matéria-prima – são tecnologias “para agir sobre a informação”, e não apenas informação para agir sobre a tecnologia; ii) Sendo a informação uma parte integral da vida humana, há uma “penetrabilidade dos efeitos das novas tecnologias”, sendo que nossa existência acaba por ser moldada pelo novo meio tecnológico⁸⁴; iii) As novas tecnologias da informação funcionam conforme a “lógica de redes”, que é próprio de qualquer sistema ou conjunto de relações que utilizam as tecnologias da informação, bem como permite crescimentos exponenciais⁸⁵; iv) Os processos, organizações e instituições podem ser modificadas, alteradas e reorganizadas em seus componentes, demonstrando o aspecto da “flexibilidade” que assume o paradigma da tecnologia da informação⁸⁶; v) A revolução das TICs, conforme já analisado, tem característica de uma crescente “convergência das tecnologias específicas para um sistema altamente integrado”, ou seja, ela se torna potencialmente ubíqua e impossível de se distinguir em separado, seja por integração de empresas, alianças estratégicas, projetos de cooperação e, mais recentemente, a convergência entre a biologia e a microeletrônica.⁸⁷ Por fim, para Christopher Freeman, essa mudança contemporânea de paradigma pode ser vista como uma “transferência da tecnologia baseada em insumos baratos de energia para uma outra que se baseia predominantemente em insumos baratos de informação derivados do avanço da tecnologia em microeletrônica e telecomunicações”.⁸⁸

Dessa forma, vive-se um momento raro na história, um intervalo cuja principal característica é a transformação da nossa "cultura material". Isso se dá pelos mecanismos de um novo paradigma tecnológico organizado da informação

⁸⁴ Assim, riscos são potencialmente criados para o indivíduo, mas também para toda a coletividade.

⁸⁵ A lógica de redes penaliza aqueles que estão fora dela, são pessoas que ficam a margem do sistema, invisíveis. As redes são criadas não só para se comunicar, mas para ganhar posições, melhorar a comunicação. A formação de novos processos e formas sociais, são facilitados pela tecnologia, mas ainda não é certa a consequências que essas interações poderão ocasionar. Cf.: CASTELLS, *op. cit.*, p. 125.

⁸⁶ Esse aspecto pode se revelar, conforme desenvolvido por Castells, como uma característica boa e ruim, ao mesmo tempo. Boa pois a flexibilidade pode ser uma força libertadora, mas ruim se, caso os redefinidores das regras forem sempre os poderes constituídos, houver uma tendência repressiva.

⁸⁷ *ibid.*, p. 125.

⁸⁸ *ibid.*, p. 125.

e do conhecimento. Quem os controla, domina o principal fator de produção da sociedade.⁸⁹ O paradigma da tecnologia da informação é, portanto, um sistema aberto “como uma rede de acessos múltiplos. É forte e impositivo em sua materialidade, mas adaptável e aberto em seu desenvolvimento histórico. Abrangência, complexidade e disposição em forma de rede são seus principais atributos.”⁹⁰

A Sociedade Informacional proposta por Manuel Castells é um marco sociológico de inquestionável relevância. O autor cunha o termo “TICs – Tecnologias da Informação e Comunicação” e desenvolve em seu trabalho o modo como sua evolução moldou uma nova forma de sociedade pós-industrial. Há, nesse sentido, um novo capitalismo informacional, com novas relações de trabalho e de produção. Isso transforma as relações sociais e a cultura, que passam a serem estruturas em redes de informação. Mas, não obstante os inegáveis e incomparáveis progressos decorrentes dessa nova configuração social, quais são os riscos inerentes às tecnologias da informação e comunicação? Como a sociedade se relaciona com esses riscos? É possível prevê-los? Para que seja possível buscar algumas respostas para esses questionamentos, é necessário compreender outra teoria sociológica de igual importância para a sociologia – a Sociedade de Risco.

1.4. UMA MODERNIDADE REFLEXIVA: A TEORIA DA SOCIEDADE DE RISCO

Em seu livro sobre a modernização reflexiva, o sociólogo alemão Ulrich Beck estabelece como uma questão central em seu trabalho a possibilidade de a sociedade industrial estar passando por um processo de autodestruição silencioso, cujo sujeito não é uma revolução sangrenta ou crises governamentais, mas a própria vitória da modernização ocidental. Trata-se de um processo de transformação das formas sociais dessa sociedade industrial clássica para uma outra modernidade, totalmente modificada e que acaba com suas bases históricas como as formações de classe, camadas sociais, relações

⁸⁹ DOWBOR, *op. cit.*, p. 46.

⁹⁰ CASTELLS, *op. cit.*, p. 128.

entre sexos, família, agricultura e setores empresariais.⁹¹ Esse processo de transformação rompe com os pré-requisitos que foram a estrutura do progresso técnico-econômico nos séculos XIX e XX e culmina em um novo estágio da modernidade onde o progresso se torna autodestrutivo – ou seja – a modernização, ao mesmo tempo que avança, se destrói e modifica. A esse processo, Beck chama de etapa da modernização reflexiva.⁹²

O conceito de modernização reflexiva, ainda segundo o autor, refere-se à transição da sociedade industrial para a Sociedade de Risco, que é acelerado pela produção e intensificação da dinâmica de uma sociedade produtora de riscos em escala global. Isso ocorre quando mecanismos produzidos pela própria sociedade industrial deixam de considerar os perigos dos efeitos colaterais inerentes ao seu desenvolvimento e rompe com seus próprios princípios de segurança.⁹³

Nesse sentido, o que antes parecia funcional e racional, passa a ser uma ameaça à vida e ao planeta, produzindo e legitimando uma disfuncionalidade e irracionalidade da sociedade:

La modernización reflexiva contiene ambos elementos: la amenaza cuasi refleja a los propios fundamentos de la sociedad industrial mediante una triunfadora profundización de la modernización que es ciega a los peligros, y el desarrollo de la conciencia, la reflexión sobre esa situación.⁹⁴

Esse processo de transformação social decorrente da modernização pode ser dividido em duas fases. Na primeira, a sociedade produz riscos como uma consequência do desenvolvimento – são riscos necessários ao progresso, e, portanto, são auto ameaças da sociedade industrial, estágio em que ela intensifica e legitima as ameaças criados pelo processo decisório da modernização como “riscos residuais”.⁹⁵

⁹¹ BECK, Ulrich; GIDDENS, Anthony; LASH, Scott. **Modernização reflexiva**: política, tradição e estética na ordem social moderna. São Paulo: Editora da Universidade Estadual Paulista, 1997. p. 14.

⁹² BECK; GIDDENS; LASH, *op. cit.*, p. 13.

⁹³ BECK, Ulrich. **La sociedad del riesgo global**. España: Siglo Veintiuno, 2002. p. 126.

⁹⁴ Tradução livre: A modernização reflexiva contém ambos os elementos: a ameaça quase reflexa aos próprios fundamentos da sociedade industrial mediante um triunfante aprofundamento da modernização que é cega aos perigos e ao desenvolvimento da consciência e reflexão sobre essa situação. Cf.: BECK, 2002, *op. cit.*, p. 127.

⁹⁵ BECK, 2002, *op. cit.*, p. 113.

Uma situação diferente ocorre quando os perigos e riscos dessa sociedade industrial passam a dominar o debate público e privado, momento no qual as instituições passam a produzir e legitimar as ameaças que não conseguem mais controlar. É exatamente nesse contexto que Ulrich Beck define a modernização reflexiva, se referindo o termo a uma auto confrontação da sociedade industrial, ou a forma como essa sociedade percebe os riscos criados:

La transición desde la época de la modernidad industrial a la del riesgo se produce de forma no intencional, no percebida, compulsivamente, en el curso de una dinámica de la modernización que se ha hecho autónoma, siguiendo la pauta de las consecuencias no deseadas.⁹⁶

Nesse sentido, inicia-se uma transição de uma sociedade industrial para o que Ulrich Beck denominou como “Sociedade de Risco”⁹⁷. Essa passagem entre sociedades pode ser definida por uma transformação sistêmica e de época em 03 (três) áreas: 1) A relação entre a sociedade industrial moderna com os recursos naturais que são escassos, ou seja, dependem de reservas finitas; 2) A relação entre a sociedade com as ameaças produzidas por ela mesma, que transbordam a fundação de um conceito social de segurança, ou seja, ela não consegue mais controlar os riscos criados por ela mesma e; 3) O esgotamento, dissolução e desencantamento com as fontes de significado social que perduraram por séculos, como a crença no progresso, na consciência de classe e na cultura e ideais de segurança social.⁹⁸

Desse modo, Ulrich Beck teoriza sobre o desenvolvimento da Sociedade de Risco em um contexto em que as novas tecnologias criam riscos de destruição planetária em proporções catastróficas. Ao diferenciar os riscos das ameaças, ele atribuiu a geração de riscos da modernidade a um processo de irresponsabilidade organizada que envolve instituições sociais como a ciência, a política e o direito. Os riscos, nesse estágio da sociedade, passam a ter outro papel. Eles deixam de ser uma ameaça individual ou isolada, e passam a ser ameaças globais que escapam à nossa percepção:

⁹⁶ Tradução livre: A transição desde a época da modernidade industrial a do risco se produz de forma não intencional, não percebida, compulsivamente, no curso de uma dinâmica de modernização que se fez autônoma, seguindo a pauta das consequências não desejada. Cf.: BECK, 2002, *op. cit.*, p. 114.

⁹⁷ O termo refere-se a um momento histórico em que há uma ruptura nos contornos da sociedade industrial clássica, dando luz a uma nova forma social, denominada pelo autor como “Sociedade de Risco”. Cf.: BECK, 2015, *op. cit.*, p. 12.

⁹⁸ BECK, 2002, *op. cit.*, p. 117.

Os riscos e ameaças atuais diferenciam-se, portanto, de seus equivalentes medievais, com frequência semelhante por fora, fundamentalmente por conta da globalidade de seu alcance (ser humano, fauna, flora) e de suas causas modernas. São riscos da modernização. São um produto de série do maquinário industrial do progresso, sendo sistematicamente agravados com seu desenvolvimento ulterior.⁹⁹

Enquanto ameaças e incertezas são condições gerais da existência humana, o risco está relacionado diretamente com o seu processo de modernização. A transição da sociedade industrial para a Sociedade de Risco ocorre quando as certezas da sociedade industrial, ou seja, tudo aquilo que lhe confere sentido, passam a ser abstraídos dos seus potenciais efeitos e riscos para a humanidade. Como consequência, o debate sobre os riscos passa a dominar o pensamento e a ação das pessoas e instituições. A Sociedade de Risco surge despercebida e o seu aparecimento não é uma questão de escolha, pois "ela surge na continuidade dos processos de modernização autônoma, que são cegos e surdos a seus próprios efeitos e ameaças".¹⁰⁰

A Sociedade de Risco, portanto, é uma teoria que visa estudar o processo de modernização conforme se dá o desenvolvimento da sociedade industrial que passa por um processo de modernização que se torna "reflexivo"¹⁰¹. Trata-se de uma das principais teorias modernas que visam explicar o modo como a sociedade se relaciona com os riscos criados pelo progresso. Ulrich Beck buscou evidenciar uma transição da era moderna para a pós-moderna por meio dos impactos socioambientais derivados de processos político-científicos de tomadas de decisão que, especialmente no contexto das revoluções industriais, deixou de considerar os seus efeitos – ou seja – os riscos derivados do processo de modernização.¹⁰² Assim, o compromisso com um "futuro próspero" da sociedade deu lugar a um contexto de insegurança social, expondo que os avanços da ciência, indústria e tecnologia, embora sejam essenciais para o desenvolvimento humano, se mostraram ambivalentes, ou seja, capazes de

⁹⁹ BECK, 2015, *op. cit.*, p. 26.

¹⁰⁰ BECK; GIDDENS; LASH, *op. cit.*, p. 18.

¹⁰¹ Reflexivo, conforme já abordado no presente trabalho, se relaciona ao processo no qual o desenvolvimento da sociedade se torna razão de sua própria instabilidade.

¹⁰² BECK, 2015. *op. cit.*, pp. 22-25.

provocar riscos que, antes, eram inimagináveis para a sociedade e para o meio ambiente.¹⁰³

Nessa toada, Beck trabalha a relação entre a Sociedade de Risco e o estado de bem-estar, analisando como o processo de transformação da sociedade industrial, que trabalhava com riscos residuais, se transformou na Sociedade de Risco, que trabalha com riscos que não podem mais serem controlados. Como analisado no capítulo 2 (dois), a sociedade industrial se transforma involuntariamente em uma Sociedade de Risco pelos seus próprios riscos sistematicamente produzidos, em um contexto de racionalidade econômica. Nesse contexto, se tais perigos são eventualmente identificados, combate-se seus sintomas, mas nunca suas causas, vez que isso se traduziria em uma luta da sociedade industrial contra si mesma.¹⁰⁴

Assim, o autor objetiva com sua pesquisa desenvolver uma teoria que permita tornar visível “um futuro que já se anuncia no presente”¹⁰⁵, ou como as instituições políticas da sociedade industrial contribuíram – e continuam contribuindo – para a criação das incertezas e riscos sociais. Esse processo, segundo ele, é resultado de decisões humanas que afetam indivíduos e se tornam, assim, riscos.¹⁰⁶

Esses efeitos indesejáveis criados pelo processo de modernização normalmente são determinados como consequências necessárias para o desenvolvimento econômico, bem como para a concretização das promessas de bem-estar da civilização. Trata-se, em verdade, de um contrato de risco, onde o desenvolvimento da sociedade fica vinculado à criação inevitável de riscos¹⁰⁷, mas que eventualmente serão submetidos à regras de prevenção e compensação, com ferramentas de gestão de risco e contratos de seguro.¹⁰⁸

¹⁰³ FERREIRA, Helene Sivini. **A biossegurança dos organismos transgênicos no direito ambiental brasileiro**: uma análise fundamentada na teoria da sociedade de risco. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina, CPGD, 2008. p. 27.

¹⁰⁴ BECK, 2002, *op. cit.*, p. 135.

¹⁰⁵ Segundo o autor, trata-se de uma teoria social prospectiva, empiricamente orientada. Cf.: BECK, 2015, *op. cit.*, p. 11.

¹⁰⁶ Nesse sentido, eles são acontecimentos sistêmicos, passíveis de descrição estatísticas, e, portanto, calculáveis, podendo ser submetidos a regras de compensação e de prevenção acima do nível individual. (*ibid.*, p. 27),

¹⁰⁷ Essa é uma invenção social muito conhecida desde os primórdios da navegação mercante internacional, quando inúmeros desbravadores se arriscavam em viagens marítimas em busca de riquezas.

¹⁰⁸ BECK, 2015, *op. cit.*, p. 27.

Segundo Heline Sivini Ferreira, embora essa concepção de desenvolvimento econômico sem levar em conta suas consequências tenha perdurado (ou ainda perdure) por décadas, há constatações empíricas de que “o crescimento econômico não é necessariamente sinônimo de desenvolvimento, especialmente quando este é considerado em sentido amplo”. Sem levar em conta as consequências e criação de riscos para o processo de desenvolvimento, os efeitos negativos são perpetuados pelo processo de modernização, gerando um processo de crise generalizada.¹⁰⁹

Para Ulrich Beck, essa transformação social ocorre a partir da passagem da sociedade industrial clássica do século XIX, denominada pelo autor como “Primeira Modernidade” ou “Modernidade Simples” para a “Segunda Modernidade”, também denominada como “Sociedade de Risco”¹¹⁰ do final do século XX e início do século XXI. A primeira modernidade, que em sua concepção dissolveu a sociedade feudal agrária, também foi dissolvida pela atual modernidade, marcada pelo intenso avanço tecnológico e dos processos produtivos.¹¹¹

Segundo a teoria do sociólogo alemão, a evolução da sociedade pode ser organizada em 03 (três) fases: (i) sociedade pré-industrial, (ii) sociedade industrial e (iii) Sociedade de Risco. A primeira tem como principal característica a presença de perigos “incalculáveis” como a fome, enchentes e outras ações da natureza até então pouco compreendidas. Esses perigos não deixam de existir, mas somam-se aos novos riscos criados pelo desenvolvimento humano. Na sociedade industrial, por sua vez, passa-se a combinar as duas espécies de ameaças: riscos produzidos pelas ações humanas e os já elencados perigos da

¹⁰⁹ FERREIRA, 2008, *op. cit.*, p. 28.

¹¹⁰ De forma objetiva, a Sociedade de Rico pode ser definida como: i) uma sociedade catastrófica, em que o estado de emergência ameaça tornar-se o estado normal; ii) O risco relativiza a posição de classe, ou seja, atinge pobres e ricos, seja em relação aos riscos ecológicos, mas também em relação aos ricos derivados de uma sociedade altamente conectada; iii) A produção de riscos não contradiz a lógica de valorização do capital, muito pelo contrário, há um aproveitamento econômico dos riscos; iv) O risco ressalta o papel da consciência e exige da sociologia contribuição para uma teoria do surgimento e divulgação da consciência do risco.

¹¹¹ PINTO, Celciane Malcher. A sociedade de risco na visão de Ulrich Beck e suas conexões com o direito e meio ambiente. **Revista de Direito e Sustentabilidade**. Encontro Virtual, v. 7, n. 1, p. 73-91, Jan/Jul. 2021. e-ISSN: 2525-9687. p. 75

natureza. A principal característica dessa sociedade é que os riscos são calculáveis e previsíveis.¹¹²

No entanto, foi o estado de autolimitação da sociedade industrial, junto ao processo de modernização, que fez nascer a Sociedade de Risco, que se origina “quando os riscos oriundos de ações e decisões humanas rompem os pilares de certeza estabelecidos pela sociedade industrial, minando, como consequência, os seus padrões de segurança”.¹¹³ Essas ameaças, criadas pela sociedade industrial, se tornam cada vez mais evidentes como o resultado do processo de modernização, extrapolando as fronteiras nacionais e culminando em consequências que afetam toda a humanidade, independente da sua localização espacial ou classe social. Ulrich Beck cita como exemplo os “mega perigos” nucleares, químicos, genéticos e ecológicos que provocam riscos globais, muitas vezes irreparáveis e impossíveis de serem limitados.¹¹⁴

Embora haja uma predominância de estudos que relacionem esses efeitos negativos do processo de desenvolvimento da sociedade industrial com a temática ambiental, essas consequências também recaem especialmente sobre os homens, notadamente em relação aos seus direitos da personalidade com o uso de tecnologias da informação e comunicação que processam uma quantidade cada vez maior de dados pessoais, por vezes de forma imperceptível e com consequências severas ao desenvolvimento da personalidade humana:

E assim como ambientalistas seguem a anos nos alertando das consequências do uso exacerbado dos combustíveis fósseis, os pesquisadores que estudam as intersecções da tecnologia e sociedade voltam-se cada vez mais para as consequências sociais da exploração do Big Data pelas grandes empresas na corrida pela extração desses bens imateriais.¹¹⁵

Por conseguinte, Beck desenvolve a tese de que a sociedade industrial passa a criar riscos de destruição planetária a partir do momento em que se

¹¹² CAVEDON, Ricardo; FERREIRA, Helene Sivini; FREITAS, Cinthia Obladen de Almendra. A dimensão ambiental da teoria da Sociedade de Risco. In: FERREIRA, Helene Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). **Direito Socioambiental e Sustentabilidade**: Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016. p. 198.

¹¹³ *ibid.*, p. 199.

¹¹⁴ BECK, 2002, *op. cit.*, p. 84.

¹¹⁵ MACHADO, Débora. A modulação de comportamento nas plataformas de mídias sociais. In: **Sociedade de Controle**: Manipulação e modulação nas redes digitais. 1. ed. São Paulo, SP. Hedra, 2018a. p. 47.

perde a possibilidade de controlar os riscos criados pelo processo de modernização:

No sentido de uma teoria social e de um diagnóstico de cultura, o conceito de Sociedade de Risco designa um estágio da modernidade em que começam a tomar corpo as ameaças produzidas até então no caminho da sociedade industrial. Isto levanta a questão da autolimitação daquele desenvolvimento, assim como a tarefa de redeterminar os padrões (de responsabilidade, segurança, controle, limitação do dano e distribuição das consequências do dano) atingidos até aquele momento, levando em conta as ameaças potenciais.¹¹⁶

Essa transição entre sociedade industrial e Sociedade de Risco faz com que os próprios limites do desenvolvimento capitalista sejam confrontados. Na primeira modernidade (ou sociedade industrial clássica), os riscos eram aceitos como uma consequência necessária do progresso, enquanto na segunda modernidade (Sociedade de Risco), eles já não podem ser percebidos como um fator inevitável do processo de modernização.

Nesse sentido, a teoria da Sociedade de Risco estabelece, como concepção inicial, a criação de riscos essencialmente ecológicos, enfrentando a possibilidade de destruição de toda a vida do planeta conforme ocorram os avanços de uma sociedade industrializada e tecnológica¹¹⁷. Pode-se entender que essa nova modernidade, marcada pelos avanços tecnológicos a partir do século XX, também é caracterizada pelo surgimento de novos riscos ambientais, sociais, políticos e econômicos que são, na maioria das vezes, imprevisíveis e abstratos, os tornando insuscetíveis ao controle das instituições.¹¹⁸

Isso é especialmente problemático quando as ameaças passam a escapar da percepção sensorial das pessoas¹¹⁹, ou seja, são riscos invisíveis e,

¹¹⁶ BECK, 1997 *apud* PINTO, *op. cit.*, p. 75.

¹¹⁷ Nota-se essa concepção da Sociedade de Risco essencialmente vinculada ao meio ambiente ecológico no seguinte trecho extraído da referida obra: "Riscos, da maneira como são produzidos no estágio mais avançado do desenvolvimento das forças produtivas – refiro-me, em primeira linha, à radioatividade, que escapa completamente à percepção humana imediata, mas também às toxinas e poluentes presentes no ar, na água e nos alimentos e aos efeitos de curto e longo prazo deles decorrentes sobre plantas, animais e seres humanos -, diferenciam-se claramente das riquezas. Eles desencadeiam danos sistematicamente definidos, por vezes irreversíveis, permanecem no mais faz vezes fundamentalmente invisíveis, baseiam-se em interpretações causais, apresentam-se, portanto, tão somente no conhecimento (científico ou anticientífico) que se tenha deles, podem ser alterados, diminuídos ou aumentados, dramatizados ou minimizados no âmbito do conhecimento e estão, assim, em certa medida, abertos a processos sociais de definição. Dessa forma, instrumentos e posições da definição dos riscos tornam-se posições-chave em termos sociopolíticos. Cf.: BECK, 2015, *op. cit.*, p. 27.

¹¹⁸ BECK, 2015, *op. cit.*, pp. 29-30.

¹¹⁹ BECK; GIDDENS; LASH, *op. cit.*, p. 19,

por vezes, com aparência inofensiva, mas que na verdade passam a ditar as nossas vidas por meio da modulação do nosso comportamento, recorrendo a um intenso conjunto de tecnologias e tratamento de dados pessoais com finalidades pouco transparentes.¹²⁰

Helene Sivini Ferreira trata o problema do desenvolvimento insustentável como a relação direta entre o desenvolvimento das ciências e técnicas com a criação de ameaças e riscos:

Talvez a humanidade até tenha subestimado o aumento do seu poder de destruição por um certo tempo. No contexto da modernidade avançada, todavia, essa assertiva carece de qualquer validade. Nas palavras de Morin e Kern (2003, p. 91), “o mito do progresso hoje desmorona, o desenvolvimento está enfermo; todas as ameaças para o conjunto da humanidade têm pelo menos uma de suas causas no desenvolvimento das ciências e técnicas”. Apesar disso, o homem continua a investir na sua força de dominação e treinar a sua capacidade de transformar, reproduzir e recriar, sem impor qualquer limitação à sua pretensão de tudo conhecer. As variações qualitativas na natureza do risco, no entanto, evidenciam que se está diante de um modelo de desenvolvimento insustentável sob os mais variados aspectos, inclusive porque envolve riscos que solapam os padrões de segurança não apenas pela sua complexidade, mas também pela sua imperceptibilidade.¹²¹

Há, a partir da perpetuação desse modelo sistemático de criação de riscos, um processo de questionamento da sociedade em relação a ideia de possibilidade de controle em relação às ameaças criadas pelo processo de modernização. Nesse sentido, a Sociedade de Risco pode ser retratada como um resumo de uma época em que há uma predominância de incertezas em relação aos riscos criados pelo processo de modernização, já que há ameaças que atingem a todos e não podem mais ser controlados ou evitados.¹²²

E, assim, a Sociedade de Risco nasce conforme se evidencia o estado de autolimitação da sociedade industrial, impulsionado pelos avanços tecnológicos, industriais e científicos e acelerado pelo desenvolvimento econômico. Juntam-se às ameaças da primeira modernidade, ainda previsíveis e calculáveis, os da segunda modernidade – os imprevisíveis e incalculáveis, que são frutos de ações e decisões humanas, rompendo com os fundamentos de certeza estabelecidos

¹²⁰ É o caso das plataformas e redes sociais que filtram a comunicação dos seus usuários, analisam os seus comportamentos e os inserem em bolhas de pessoas com perfis semelhantes.

¹²¹ FERREIRA, 2008, *op. cit.*, p. 37.

¹²² BECK, 2015, *op. cit.*, p. 29.

pela sociedade industrial e “minando, como consequência, os seus padrões de segurança”.¹²³

Posto isto, até que ponto essa nova sociedade informacional, como a proposta pelo sociólogo Manuel Castells e analisada nos tópicos anteriores, desempenhou (ou desempenha) um papel relevante no desenvolvimento da Sociedade de Risco conforme proposto por Ulrich Beck? Se no passado riscos já existiam, a universalização do conhecimento sobre esses riscos por meio das TICs gera um impacto negativo na visão das pessoas sobre o mundo, especialmente com os meios de comunicação de massa que atualizam todos de forma instantânea, aumentando o grau de ansiedade das pessoas.¹²⁴

Nesse sentido, o risco pode ser sinteticamente definido com um perigo possível que se projeta no futuro por escolhas do presente¹²⁵. Segundo Heline Sivini Ferreira, em seu artigo intitulado “A dimensão ambiental da Sociedade de Risco”, o risco “encontra-se fortemente vinculado às noções de probabilidade e incerteza”.¹²⁶ Ele está, portanto, vinculado ao futuro, sendo percebido por meio da probabilidade – se alguma coisa é mais ou menos provável de acontecer, a partir de observações no presente ou passado. Nesse caso, se a probabilidade de um evento ocorrer é alta, tem-se o risco. Se a chance é baixa, tem-se a incerteza. Tal incerteza, todavia, não constitui, necessariamente, um risco. Para isso, é necessário que ela “impacte de alguma forma a realidade humana”.¹²⁷

Não obstante, o risco não é sinônimo de perigo. Enquanto o último tinha causas essencialmente naturais, não importando a sua dimensão – eram “golpes do destino que se descarregavam sobre a humanidade a partir de fora, sendo

¹²³ FERREIRA, 2008, *op cit.*, p. 37.

¹²⁴ LITTLE, Josh. Risk in the age of information. **Critical Reflections: A Student Journal on Contemporary Sociological Issues**, 2018. Disponível em: <https://ojs.leedsbeckett.ac.uk/index.php/SOC/article/view/4547>. Acesso em: 6 nov. 2022.

¹²⁵ Esse conjunto de decisões envolve probabilidades que são incertas não apenas quanto à sua ocorrência, mas também quanto à sua dimensão. Cf.: FERREIRA, 2008, *op cit.*, p. 34.

¹²⁶ FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). **Direito Socioambiental e Sustentabilidade: Estados, Sociedades e Meio Ambiente**. Curitiba: Letra da Lei, 2016. p.110.

¹²⁷ Embora haja um exercício de tentativa para definição do risco, tal conceituação pode não ser recomendada, dadas as suas diferentes características conforme o tempo e o contexto social de análise. Todavia, o risco normalmente está relacionado ao “prenúncio ou indício de uma ameaça ou perigo”. Nesse sentido, o risco é comumente relacionado com o mundo econômico por meio dos cálculos estatísticos para viabilizar a tomada de decisão no mercado de capitais. Cf.: FERREIRA, 2008, *op. cit.*, p. 32.

atribuíveis a um outro”¹²⁸, os riscos, por sua vez, surgem a partir do momento em que os seres humanos passam a interferir no curso da natureza.¹²⁹ Os riscos são frutos de uma construção cognitiva e social, ou seja, são objeto de um processo de racionalização¹³⁰. Eles são sistematicamente produzidos no contexto da sociedade industrial de racionalidade econômica, passando os limites do que é aceitável ou seguro.¹³¹ Isso caracteriza uma fase da modernidade em que “a interpretação das ameaças se desvincula das causas naturais e intervenções divinas para vincular-se aos processos de tomada de decisões.”¹³²

Conforme se desenrola o processo de modernização, tais características dos perigos naturais começam a se fundir com os riscos produzidos pelas ações e decisões humanas:

Outrora vinculadas tão somente ao destino, as ameaças passam a agregar também a dimensão dos riscos fabricados, ou seja, produzidos pela própria humanidade. Neste estágio, fala-se sobre riscos calculáveis cujos potenciais efeitos podem ser contidos. Essa idéia de controle racional dos acontecimentos se expande, fazendo surgir uma diversidade de sistemas de seguro e transformando a sociedade em um grupo de risco previdente (MYTHEN, 2004; BECK, 1998b).¹³³

O risco, portanto, é fruto de decisões e atividades humanas, enquanto o perigo é derivado de processos essencialmente naturais.¹³⁴ Assim, com a fabricação de riscos pela própria humanidade, passa-se a falar em “riscos calculáveis cujos potenciais efeitos podem ser contidos”¹³⁵. Essa concepção de controle racional dos riscos favorece o surgimento dos sistemas de seguros, evidenciando a legitimação do modelo de desenvolvimento econômico da sociedade criador de riscos, mas sem antes ter um “aparato cognitivo e institucional que garanta o seu controle”, ou seja, que permita que a sociedade

¹²⁸ FERREIRA, 2008, *op. cit.*, p. 36.

¹²⁹ PARDO, José Esteve. **Técnica, riesgo y derecho**. Barcelona: Ariel, 1999. p. 25.

¹³⁰ FERREIRA, 2008, *op. cit.*, p. 35.

¹³¹ BECK, 2002, *op. cit.*, p. 121.

¹³² FERREIRA, 2008, *op. cit.*, p. 35.

¹³³ *ibid.*, p.36.

¹³⁴ Segundo Heline, “As decisões e atividades humanas, associadas à inovação científico-tecnológica e ao desenvolvimento econômico, continuam a produzir riscos, e estes são propriamente os frutos da modernidade avançada.” (*ibid.*, p.35).

¹³⁵ *ibid.*, p.37.

lide consigo mesma na tentativa de reduzir os efeitos negativos resultado de suas escolhas.¹³⁶

Por fim, há uma inversão na lógica capitalista de distribuição de riquezas, exemplificada na sociedade industrial pela distribuição de bens como a renda e emprego. Na Sociedade de Risco ela se inverte, passando a haver, ao invés da distribuição de riquezas, a distribuição de riscos.¹³⁷ Isto é, há distribuição dos malefícios criados pelo processo de modernização – como a produção de bens de consumo e informação – para toda a sociedade.¹³⁸ Esses males derivados do processo de desenvolvimento passam a ser distribuídos, provocando uma crise no funcionamento da sociedade industrial.

1.5. A CONFIGURAÇÃO DA SOCIEDADE DE RISCO E A CONSTRUÇÃO INSTITUCIONAL DO RISCO

São 03 (três) os principais elementos que se relacionam e configuram a Sociedade de Risco: o risco, espaço e tempo. Se antes a sociedade industrial estava vinculada a fenômenos bem delimitados no espaço geográfico e no tempo, com a transição para a Sociedade de Risco novos fenômenos, mais complexos, são agregados aos já existentes. Disso, surgem novas peculiaridades e riscos que, ao contrário do modelo anterior, passam a “transcender os limites temporais e espaciais até então estabelecidos”.¹³⁹ Se os riscos da segunda modernidade já não podem ser definidos e contidos em limites espaciais e temporais, seus impactos também passam a ser imprevisíveis, podendo afetar a humanidade como um todo, inclusive em relação às futuras gerações. Ou seja, os novos riscos revelam um grande potencial de destruição, como nunca antes na história, bem como revela seu caráter de ameaça global.¹⁴⁰

Outro elemento que configura a Sociedade de Risco é a falência dos padrões sociais de segurança, consequência de um processo de modernização

¹³⁶ *ibid.*, p.37.

¹³⁷ BECK, 2015, *op. cit.*, p. 15.

¹³⁸ BECK; GIDDENS; LASH, *op. cit.*, p. 19.

¹³⁹ FERREIRA, 2008, *op. cit.*, p. 40.

¹⁴⁰ *ibid.*, p. 40.

acelerado que influi negativamente na noção de segurança e controle de resultados, diminuindo a proteção à medida que se aumentam os riscos¹⁴¹:

A falência dos padrões de segurança mencionada por Curbet (2002) é propriamente o terceiro elemento de configuração da Sociedade de Risco a que se pretende fazer referência. Em uma sucinta descrição da sociedade contemporânea, Beck (1998b) considera tratar-se de uma fase do desenvolvimento da sociedade moderna na qual os riscos, criados durante o acelerado processo de modernização, tornam-se predominantes e já não podem ser adequadamente controlados pelas instituições que serviram à sociedade industrial.¹⁴²

Por fim, Beck elenca como terceira característica dessa Sociedade de Risco a noção de globalidade dos riscos, resultado de um complexo emaranhado de múltiplas crises que, embora independentes em relação à sua nacionalidade, são compartilhadas por toda a humanidade em diferentes níveis. Por esse ângulo, perde-se a característica das fronteiras nacionais criadas pela humanidade, sendo que as ameaças da Sociedade de Risco não ameaçam apenas um espaço delimitado no planeta terra, mas contextos e localidades verdadeiramente globais, característica compartilhada com a noção de sociedade em rede de Castells. Soma-se a isso a predominância dos riscos criados pelo processo acelerado de modernização que culmina na perda do seu controle pelas instituições que serviram à sociedade industrial.¹⁴³ Tais elementos da Sociedade de Risco evidenciam que os riscos individuais, sociais, políticos e econômicos tendem a, cada vez mais, escapar do controle das instituições tradicionais, mas não só isso – as instituições passam a fazer parte de um esforço de reinterpretação dos riscos, na tentativa de acobertar suas reais consequências.¹⁴⁴

Helene Sivini Ferreira afirma que a análise dessa “construção institucional do risco” passa por um exame dos mecanismos de definição conforme a evolução da sociedade. Segundo Mythen¹⁴⁵, essas relações, quando definidas coletivamente, deveriam constituir recursos primários de determinação,

¹⁴¹ FERREIRA, 2016, *op. cit.*, pp. 108-158.

¹⁴² FERREIRA, 2008, *op. cit.*, p. 43.

¹⁴³ Ulrich Beck afirma que estas ameaças têm invalidado os métodos de avaliação de riscos, pois as medidas preventivas se mostram ineficazes perante a possibilidade de catástrofes significativas, prejudicando a sensação de segurança e controle dos resultados. Além disso, com riscos globais e móveis cujos danos são frequentemente irreversíveis, a abordagem convencional de indenização financeira parece ser insuficiente. Cf.: FERREIRA, 2008, *op. cit.*, p. 45.

¹⁴⁴ BECK; GIDDENS; LASH, *op. cit.*, p. 17.

¹⁴⁵ FERREIRA, 2016, *op. cit.*, pp. 108-158.

organização e regulação do risco, mas são as definições institucionais as que normalmente informam e influenciam a interpretação pública do risco, sendo por esse motivo que essa construção institucional seja um dos principais instrumentos de poder da segunda modernidade:

Nesse sentido, parece oportuno mencionar que se trata de um processo com dupla função: ao mesmo tempo em que orienta as atividades de criação, organização, regulação e controle das ameaças, propõe-se a garantir a existência de padrões de segurança adequados para manter os riscos isolados do domínio público. Assim sendo, afirma Beck (1995), as relações de definição podem ser consideradas como princípios básicos que fundamentam a política, a ciência, o direito, a produção industrial e as oportunidades para o público.¹⁴⁶

Se na sociedade industrial os riscos são definidos conforme uma escala de cálculos e probabilidades, na transição para a Sociedade de Risco, essa metodologia já não é válida para avaliar e controlar os riscos, resultando na falência dos padrões de segurança consolidados da sociedade industrial.¹⁴⁷ Nesse contexto, e apesar desse processo falimentar dos padrões de segurança, continua égide a necessidade de garantir a continuidade do desenvolvimento científico, tecnológico e industrial. Para isso, sobrevém a penetração dos valores alicerces da Sociedade de Risco também no campo de atuação da ciência, da política e do direito, com a dissimulação e desvirtuação das ameaças fabricadas pelo processo de modernização:

De fato, considerando que as instituições sociais repousam sobre o consentimento público, a dissimulação e o desvirtuamento das situações de risco convertem-se em um interesse institucional de primeira importância. Isso porque, como assinala Beck (1995), aceitar a responsabilidade pela produção dos riscos e admitir a falta de habilidade para contê-los conduziria certamente a uma crise de legitimação.¹⁴⁸

É nessa tensão que nasce a noção de irresponsabilidade organizada, conceito que abrange a tentativa das instituições dominantes de ocultar a realidade dos riscos por meio do exercício simbólico da ciência e do uso simbólico da política e do direito. Trata-se de um fenômeno de tentativa de acobertamento da realidade do risco, porém sem desprender-se das relações de definição que são pilares da sociedade industrial. Ou seja, apesar dos riscos não

¹⁴⁶ FERREIRA, 2016, *op. cit.*, p.129.

¹⁴⁷ FERREIRA, 2016, *op. cit.*, p.130.

¹⁴⁸ FERREIRA, 2008, *op. cit.*, p. 52.

serem mais suscetíveis à previsão ou cálculo, é por essas regras que eles continuam sendo definidos e percebidos, “sem que seja possível, contudo, garantir os padrões de segurança necessários para isolar os riscos e mantê-los afastados do domínio público.”¹⁴⁹

1.6. UMA NOVA MODERNIDADE A PARTIR DE ULRICH BECK

A Sociedade de Risco é, portanto, uma nova modernidade que cresce na consciência coletiva conforme crescem os riscos oriundos dos processos de tomada de decisão da segunda modernidade. Nesse estágio, a sociedade se transforma em um laboratório, e o progresso tecnológico, por potencializar riscos globais e catastróficos, se converte em um problema de natureza coletiva.¹⁵⁰

No âmago dessa sociedade está a corrida inevitável do progresso e do poder do homem sobre todas as outras coisas. Conforme a humanidade se desenvolve, situações inéditas criam novas ameaças que, por serem inéditas, não podem ser previstas ou controladas.¹⁵¹ Essa sociedade, enebriada pelo contexto histórico que prometeu um estado de bem-estar social e seus contratos de seguro, é, na verdade, uma sociedade sem cobertura alguma, completamente exposta aos riscos globais, mas sem pistas do perigo a que está exposta.¹⁵²

A Sociedade de Risco é uma sociedade de perigos mundiais, com consequências não restritas a fronteiras nacionais. Ela é democrática, pois afeta todos, independente da classe social. Os mercados podem entrar em colapso, bem como o sistema jurídico se mostra insuficiente para determinar os fatos. A ciência, embora torne os riscos mais visíveis, não é capaz de reduzi-los, pois está intimamente ligada com sua produção sistemática. A existência humana passa a ser determinada pelo medo, fazendo com que a segurança se torne um produto essencial e de alto valor agregado. Cria-se, assim, a economia do medo, com cidadãos agradecidos por estarem sujeitos à vigilância e controles constantes, seja do setor público ou privado. A Sociedade de Risco acaba por

¹⁴⁹ FERREIRA, 2016, *op. cit.*, pp. 108-158.

¹⁵⁰ BECK, 2002, *op. cit.*, p. 130.

¹⁵¹ *ibid.*, p. 137.

¹⁵² *ibid.*, p. 133.

negar os princípios da sua racionalidade, pois ela opera além do que é considerado seguro.¹⁵³

Apesar da visão catastrófica provocada pela concepção da Sociedade de Risco, como é possível repartir os riscos criados pelo processo de modernização sem criar obstáculos para o desenvolvimento econômico ou ultrapassar os limites do aceitável e suportável para a sociedade? Os interesses econômicos do capitalismo informacional são conciliáveis com o controle da criação sistemática de riscos? Ulrich Beck, em sua tentativa de buscar respostas para o problema da Sociedade de Risco, destaca a função e a influência dos movimentos sociais para a percepção dos riscos da modernidade e conclui que deve haver uma democratização das discussões envolvendo a análise de riscos das tecnologias e da ciência, envolvendo grupos de pessoas com formação interdisciplinar e ampla exposição dos meios de comunicação para que esse tema seja devidamente analisado.

¹⁵³ *ibid.*, p. 141.

2. HIPERCONNECTIVIDADE NA SOCIEDADE INFORMACIONAL E OS RISCOS À PRIVACIDADE

A hiperconectividade é um fenômeno que se manifesta na Sociedade Informacional, caracterizada pelo aumento da interconexão e interdependência entre indivíduos, organizações e governos por meio de objetos físicos, sensores, algoritmos, *Big Data*, Inteligência Artificial, entre outras tecnologias da informação. Com o advento da Internet e o crescente uso de dispositivos móveis, esse fenômeno está cada vez mais presente na vida cotidiana das pessoas. O aumento de dispositivos inteligentes e conectados passaram a gerar um fluxo contínuo de informações e tratamento massivo de dados pessoais.¹⁵⁴

No Brasil, qualquer operação de tratamento de dados pessoais, seja ela realizada por organização pública ou privada, é regulada pela Lei n° 13.709/2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD).

Segundo o art. 5°, inciso X da referida legislação, há tratamento de dados quando houver qualquer operação que envolva, por exemplo, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão, extração, entre outras operações que utilizam dados pessoais em seu ciclo de vida.

Nesse sentido, qualquer operação de tratamento realizada com dados pessoais se enquadra no conceito de tratamento da legislação brasileira de proteção de dados. Sendo assim, e considerando a realidade hiperconectada em que se vive na Sociedade Informacional, há uma infinidade de operações de tratamento que ocorrem e impactam os indivíduos a todo momento.

Tais operações criam riscos que podem assumir diferentes características. O uso de dados pessoais em velocidade, volume e variedades cada vez maiores¹⁵⁵ fazem surgir, por exemplo, diversos riscos à privacidade,

¹⁵⁴ MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019. p. 20.

¹⁵⁵ Essas características também estão presentes no tratamento de dados em *Big Data*, que pode ser definido como um conjunto de dados maior e mais complexo, especialmente de novas fontes de dados. Esses conjuntos de dados são tão volumosos que o software tradicional de processamento de dados simplesmente não consegue gerenciá-los. O termo normalmente está

sendo esse um direito fundamental protegido pela Constituição da República Federativa do Brasil de 1988 (CRFB) em seu artigo 5º, inciso X e LXXIX.

À medida em que se torna cada vez mais difícil precisar quando, onde, como, por quem e por que os dados são tratados, também se torna desafiador controlar a utilização de ferramentas que, recorrendo a diversos tipos de tratamento de dados – inclusive de maneira automatizada, classificam e definem quem terá acesso à serviços e produtos, bem como personalizam anúncios e determinam quais notícias e atualizações em *feeds* de redes sociais o indivíduo terá acesso.

É com essa perspectiva que potenciais riscos são criados pela Sociedade Informacional hiperconectada. Não se fala mais em tecnologias que permitem a simples comunicação entre pessoas, mas de um universo de dispositivos e redes com o potencial real de determinar o direito de acesso a determinados tipos de serviços e produtos, como, por exemplo, seguros, financiamentos e planos de saúde. Não obstante, essas tecnologias potencializam os riscos de modulação do comportamento da sociedade, especialmente após a popularização das mídias sociais.¹⁵⁶

Luciano Floridi, em seu livro *The Onlife Manifesto - Being Human in a Hyperconnected Era*, trata a ideia central de que as TICs não são meras ferramentas que podemos manejar, mas:

[...] verdadeiras forças ambientais que vêm afetando cada vez mais quatro dimensões centrais de nossas vidas: (i) nossa concepção de quem somos; (ii) nossas interações com outras pessoas; (iii) nossa concepção da realidade; (iv) nossa interação com a realidade.¹⁵⁷

Assim, conforme incorporam-se o uso dessas novas tecnologias na sociedade, por vezes com efeitos ainda mal compreendidos, passa-se a um processo cumulativo de novos perigos e riscos imprevisíveis e incalculáveis, característicos da Sociedade de Risco proposta por Ulrich Beck:

ligado à conceituação dos três Vs do Big Data: Volume, Velocidade e Variedade. Cf.: ORACLE. **O que é Big Data?** Disponível em: <https://www.oracle.com/br/big-data/what-is-big-data/>. Acesso em: 6 nov. 2022.

¹⁵⁶ MACHADO, 2018a, *op. cit.*, p. 48.

¹⁵⁷ DE SOUZA, Clarisse S. **Vida na Era da Hiperconectividade**. EMAPS-Resenhas #05. Rio de Janeiro, RJ - Brasil: SERG, Departamento de Informática, PUC-Rio, 2021. p. 15. Disponível em: <http://www.hcc.inf.puc-rio.br/EMAPS/userfiles/downloads/Resenha-Floridi2015.pdf>. Acesso em: 6 nov. 2022.

Com os constantes avanços da ciência, da tecnologia e da indústria, os riscos vão assumindo novas características. A formação da sociedade contemporânea, portanto, tem início quando os riscos deixam de ser calculáveis e seus efeitos passam a ser imprevisíveis (riscos abstratos). Aqui se acumulam novamente os perigos e os riscos, e estes últimos, entretanto, subdividem-se em dois grupos: os previsíveis e calculáveis e os imprevisíveis e incalculáveis. Isso significa que aos riscos característicos da primeira modernidade somam-se, agora, os riscos que vão delinear a segunda modernidade. Nessa perspectiva, assinala-se que a Sociedade de Risco tem origem quando as ameaças oriundas de ações e decisões humanas rompem os pilares de certeza estabelecidos pela sociedade industrial, minando, como consequência, os seus padrões de segurança.¹⁵⁸

A exemplo da informática, os riscos decorrentes do avanço das TICs, especialmente no contexto citado de hiperconectividade, também podem contribuir para o rompimento de pilares fundamentais da sociedade, especialmente em relação ao livre desenvolvimento da personalidade, conforme criam-se riscos à direitos fundamentais, notadamente a privacidade.

Castells menciona em sua obra um processo de convergência tecnológica que facilita e resulta na lógica compartilhada de geração de informação.¹⁵⁹ Essa convergência, ainda segundo o autor, conecta esse processo de evolução tecnológica das TICs com a genética, a biologia, a eletrônica e, claro, a própria informática.¹⁶⁰

Essas tecnologias acabam por integrar o mundo em enormes redes globais de “instrumentalidade”¹⁶¹, gerando comunidades virtuais com capacidades inventivas que foram responsáveis pelos grandes avanços tecnológicos do século XXI, mas que, também, passaram a gerar riscos globais, como, por exemplo, o caso das aplicações genéticas para a agroindústria:

[...] micro-organismos, alguns dos quais alterados geneticamente, foram recebendo uma série de funções, que incluíram limpar a poluição muitas vezes causadas pelas mesmas empresas e órgãos que vendiam os superorganismos. Porém, dificuldades científicas, problemas técnicos e obstáculos legais, oriundos de justificadas preocupações éticas e de segurança, retardaram a louvada revolução biotecnológica durante a década de 1980.¹⁶²

Essa relação entre inovação tecnológica e produção de riscos é a questão central da obra de Ulrich Beck. Para ele, os efeitos da modernização se

¹⁵⁸ CAVEDON; FERREIRA; FREITAS, 2015, *op. cit.*, p. 200.

¹⁵⁹ CASTELLS, *op. cit.*, p. 126.

¹⁶⁰ CASTELLS, *op. cit.*, p. 87.

¹⁶¹ CASTELLS, *op. cit.*, p. 77.

¹⁶² CASTELLS, *op. cit.*, p. 110.

precipitam em forma de ameaças a própria humanidade. Eles não podem mais ser limitados, pelo contrário. Assim como a convergência de tecnologias permitiu o seu desenvolvimento por meio de redes globais, seus efeitos e consequências também o são.¹⁶³ Assim, criam-se riscos conforme há um crescente uso das TICs e sua utilização acarreta um volume cada vez maior de processamento de dados pessoais. As eventuais consequências desse fenômeno ainda são incertas, à medida que não há instituições preparadas para lidar com os piores cenários possíveis em relação ao seu potencial lesivo.¹⁶⁴

Embora o desenvolvimento da Internet seja considerado como fator decisivo para a viabilização da Sociedade Informacional, e em consequência dos seus riscos, ela, *per se*, não deve ser considerada uma tecnologia nociva à sociedade. Todavia, foi o processo de modernização da sociedade, com a criação de uma série de tecnologias que se utilizam da Internet e realizam o tratamento de dados, que acelerou o processo de criação de riscos pela Sociedade Informacional. Nesse sentido, a dimensão digital de risco é expressa pela sociedade informacional.

A utilização dessas tecnologias por empresas e pelo poder público ainda não é um fenômeno totalmente compreendido pelos indivíduos afetados, uma vez que o tratamento de dados pelos meios digitais passa despercebido pela maioria das pessoas. Assim, o advento da Internet causa uma mudança das referências, instituições, relações de trabalho, entre outros, que podem causar um sentimento de ansiedade e perda de significado sobre a vida, retirando as premissas e instituições que deram sentido à sociedade industrial.¹⁶⁵

Nessa perspectiva, as TICs são pervasivas e ubíquas, culminando em riscos imprevisíveis e incontroláveis. Esses riscos também podem ser transfronteiriços, pois normalmente ultrapassam os limites do local originalmente impactado¹⁶⁶, e, ainda, transtemporais, pois sua criação não implica, necessariamente, num dano imediato, podendo se manifestar anos após a sua

¹⁶³ BECK, 2015, *op. cit.*, p. 16.

¹⁶⁴ FERREIRA, 2008, *op. cit.*, p. 41.

¹⁶⁵ LITTLE, *op. cit.*, p. 11

¹⁶⁶ Nesse sentido, a LGPD estabelece requisitos para a transferência internacional de dados, como a necessidade de o país receptor contar com um grau de proteção de dados previsto na legislação brasileira ou o controlador dos dados oferecer e comprovar garantias de cumprimento dos princípios da lei e dos direitos do titular de dados pessoais (Art. 33 e seguintes da LGPD).

exposição.¹⁶⁷ Quando a temática é o tratamento de dados pessoais no meio digital, a distância entre a coleta de dados e o dano pode ser de um clique.

No tópico 1.3, foi analisado que todos esses avanços culminam em uma mudança fundamental de paradigma. A humanidade passa a viver numa sociedade segundo uma lógica de redes – conectada, globalizada, capitalista, fluída, disruptiva e inovadora. Sua grande viabilizadora, sem a qual nada disso seria possível – a Internet – passa a dominar todos os aspectos políticos, econômicos e sociais do ser humano, conectando a tudo e a todos.¹⁶⁸

Nesse sentido, a rede mundial de computadores é concebida para se transformar mais recentemente em teia que une cada aspecto da nossa sociedade no século XXI. Quase como uma consequência de seu advento, nascem novas criaturas desse ambiente – como o *Big Data*, a Inteligência Artificial e outras tecnologias que passam a demandar mais e mais dados. Todas essas revoluções trouxeram inúmeros benefícios à sociedade, mas, ao mesmo passo, criaram riscos ainda pouco compreendidos.

2.1. O ADVENTO DA INTERNET E DA CONECTIVIDADE

A rede mundial de computadores, também conhecida como Internet, pode ser definida como sendo “a canalização necessária para que a informação dos mais diversos tipos possa fluir de um computador para outro por todo o planeta”¹⁶⁹. Trata-se de uma tecnologia que conecta dispositivos de diversos tipos, separados em uma rede universal, possibilitando a comunicação entre si, não importando sua localização. Sua tecnologia é baseada na troca de pacotes que, em sua gênese, teve como principal objetivo permitir a comunicação entre computadores separados em uma rede universal, sem um centro de controle e comando, sendo assim uma infraestrutura menos vulnerável a ataques – inclusive nucleares.¹⁷⁰

Embora sua origem remonte ao ano de 1958, quando o Departamento de Defesa dos Estados Unidos cria a ARPA – *Advanced Research Projects Agency*,

¹⁶⁷ CAVEDON; FERREIRA; FREITAS, *op. cit.*, p. 201.

¹⁶⁸ CASTELLS, *op. cit.*, p. 107.

¹⁶⁹ ARAYA, Erm.; VIDOTTI, Sabg. **Criação, proteção e uso legal de informação em ambientes da World Wide Web [online]**. São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2010.

¹⁷⁰ CASTELLS, *op. cit.*, p. 101.

ela de fato só foi possível graças ao desenvolvimento da própria informática¹⁷¹, que nasce após uma substancial mobilização do governo norte-americano, depois da segunda guerra mundial em sua tentativa de superar a União Soviética tecnologicamente. O fator determinante para esse investimento foi a necessidade cada vez maior de realização de cálculos com finalidades balísticas, organização logística militar, telecomunicações e o melhoramento da arma atômica.¹⁷²

Uma das principais bases conceituais da ciência computacional é a teorizada pelo matemático Alan Turing, também conhecido como o pai do computador, que afirmou que tudo aquilo que pode ser calculado, também tem condições de ser mecanizado.¹⁷³ Nesse sentido, um computador pode ser definido como uma máquina que realiza uma série de comandos previamente programados – ou seja, programas – que permitem organizar, processar ou transformar a informação.¹⁷⁴

A partir do marco histórico de Turing com sua primeira máquina capaz de executar cálculos complexos, o desenvolvimento da informática se dá por meio dos impulsos de um complexo institucional muito característico – a união da academia, o departamento de defesa dos Estados Unidos e empresas sob contrato com laboratórios governamentais. A guerra fria passa a ser o principal fator para investimentos em informática, agora não só para a realização de cálculos, mas também para auxiliar o ser humano na tomada de decisão e, especialmente, para facilitar a sua comunicação. Essa é uma importante transição que ocorre a partir da década de 1960, iniciando uma nova era na interação entre o ser humano e a máquina.¹⁷⁵

Assim, nasce a ARPA, entidade vinculada ao departamento de defesa dos Estados Unidos com a missão de coordenar os esforços de pesquisa em resposta ao programa espacial soviético.¹⁷⁶ Surge então, como uma proposta de um dos departamentos da ARPA, o *Information Processing Techniques Office*

¹⁷¹ Informática pode ser definida como a “tradução técnica de princípios de organização e de processamento da informação, baseados na digitalização”. Cf.: LOVELUCK, Benjamin. **Redes, liberdade e controle: uma genealogia política da internet**. 1. ed. São Paulo: Editora Vozes, 2018. p. 42.

¹⁷² *Ibid.*, p. 43.

¹⁷³ TURING, Alan M. Computing machinery and intelligence. **Mind**, v. 59, p. 433-460, 1950.

¹⁷⁴ LOVELUCK, *op. cit.*, p. 43.

¹⁷⁵ *Ibid.*, p. 45.

¹⁷⁶ *Ibid.*, p. 45.

(IPTO), a origem imediata da Internet, a ARPANET, denominação para *Advanced Research Projects Agency Network*. Essa rede inicialmente conectava a Universidade da Califórnia em Los Angeles, o *Stanford Research Institute*, a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah.¹⁷⁷ Trata-se da primeira rede interativa e distribuída de computadores. Sob a direção de Lawrence Roberts, seu projeto inicia-se em 1966 e é definitivamente implantado em 1969.¹⁷⁸

Todavia, quem de fato idealizou uma rede conectada de computadores, destinada e orientada à comunicação, foi o professor e pesquisador norte americano Joseph Carl Robnett Licklider, do Massachusetts Institute of Technology (MIT). Licklider foi o primeiro diretor da IPTO, e, influenciado por um projeto¹⁷⁹ para criar uma rede de alerta contra ataques de bombardeiros soviéticos, passou a desenvolver uma mudança de rumo em relação ao programa de pesquisa do IPTO, antes orientado a sistemas de controle e comando (*command and control*), para uma pesquisa que viabilizasse a criação de redes de comunicação e interação entre humanos e máquinas.¹⁸⁰

Nesse sentido, Licklider escreve o artigo em parceria com Robert Taylor denominado “*the computer as a communication device*”, apresentando os alicerces da comunicação e interação entre seres humanos e máquinas.¹⁸¹ Seu texto traz uma visão ainda romantizada da tecnologia, voltada para ideais de realização do indivíduo, criação de comunidades, aumento da eficiência e produtividade. O debate sobre as consequências do uso dessa tecnologia, especialmente em relação à democratização de acesso a essa rede “amplificadora da inteligência”, surge em um segundo momento.¹⁸²

Para que esses objetivos de utilização de computadores em rede pudessem ser atingidos, houve uma profunda modificação dos princípios e

¹⁷⁷ CASTELLS, *op. cit.*, p. 101.

¹⁷⁸ LOVELUCK, *op. cit.*, p. 46.

¹⁷⁹ Se trata do projeto Lincoln, que propunha criar um sistema em que vários radares de vigilância aérea fossem conectados e coordenados por computadores. O projeto Lincoln, de fato, resultou em um sistema que conectou 23 centros de radares, capazes de monitorar até 400 aviões de uma só vez. O sistema foi chamado de Semi-Automatic Ground Environment (SAGE), e foi a primeira rede de transferência de dados em longa distância do mundo. Cf.: ARAYA; VIDOTTI, *op. cit.*, p. 144.

¹⁸⁰ LOVELUCK, *op. cit.*, p. 46.

¹⁸¹ *Ibid.*, p. 49.

¹⁸² *Ibid.*, p. 49.

tecnologias da telecomunicação da época, ainda muito voltados para uma conexão direta, ponto a ponto.¹⁸³

É nesse contexto que é concebida a rede distribuída por comutação por pacotes (*packet switching*)¹⁸⁴, que viria a revolucionar e estabelecer um novo marco na comunicação de dados. Inicialmente, foram diversos os desafios na sua implantação, sendo ela o resultado de inúmeros desenvolvimentos dentro do IPTO, o que resultou em problemas de incompatibilidade de sistemas. Uma reestruturação ocorre em 1967 com uma medida do então diretor Larry Roberts que solicita a Lawrence Roberts um novo projeto de arquitetura de rede. A partir disso, Lawrence toma três decisões tecnológicas para desenvolver o sistema:

A primeira dessas decisões, relata Waldrop (*idem*, p.80-81), refere-se à necessidade da agência de locar uma série de linhas de telefone de longa distância e de alta capacidade que permitisse a conexão ininterrupta dos computadores com os diversos sites da Arpa, porque, como ela não disporia de recursos para ter seus próprios cabos de transmissão em todo o país, seria obrigada a realizar a transmissão de dados por meio do sistema telefônico da American Telephone and Telegraph (AT&T). Como segunda medida, Roberts decidiu que as mensagens digitais não seriam enviadas pela rede como uma corrente contínua de bits, mas, sim, segmentadas como “pacotes”, para protegê-las da estática e de distorções na linha. Essa medida, embora não eliminasse o ruído, permitiria que os erros pudessem ser isolados e assim o sistema teria a chance de arrumá-los ou de solicitar ao remetente original que enviasse uma nova cópia. A tecnologia de comutação de pacote tinha sido desenvolvida anos antes por Paul Baran, na Rand Corporation, e estudada na tese de doutorado de Leonard Kleinrock, colega de Roberts no MIT.

A terceira medida que Larry Roberts adotaria seria a completa descentralização da rede. Não haveria um computador mestre responsável pela classificação e direcionamento dos pacotes aos seus destinos.¹⁸⁵

Nasce, então, a concepção da rede distribuída, que em resumo pode ser definida como um processo de “recortar a informação em pequenos blocos e, em seguida, deixar que cada um desses pacotes encontre o melhor caminho por meio da rede, a fim de reconstruir a informação na chegada”¹⁸⁶. Isso permite o compartilhamento de pequenas quantidades de informação sem necessidade de uma conexão direta, ponto a ponto, como ocorre, por exemplo, na comutação de circuitos das antigas redes telefônicas.

¹⁸³ *Ibid.*, p. 49.

¹⁸⁴ *Ibid.*, p. 49.

¹⁸⁵ ARAYA; VIDOTTI, *op. cit.*, p. 18.

¹⁸⁶ LOVELUCK, *op. cit.*, p. 49.

Segundo Loveluck, houve um contexto social e político muito específico – o da guerra fria e a ameaça nuclear - que contribuiu para o desenvolvimento da rede distribuída. Segundo o autor, tratou-se de um “clima intelectual” que permeou não só os Estados Unidos, mas pelo menos outros três locais em que tecnologias muito semelhantes foram desenvolvidas, embora sem qualquer interação entre os pesquisadores.¹⁸⁷

Nesse sentido, é frequente o relato de que o advento da Internet é fruto de uma vontade de criar uma rede de comunicações insuscetível a ataques nucleares, mas, em verdade, a principal ideia dessa rede distribuída foi a de utilizar de forma eficiente os recursos de computação para a criação de uma comunidade de usuários. Tal objetivo acabou por utilizar uma arquitetura dotada de capacidade para conservar da melhor forma a troca de informações, mesmo que parte dela fosse destruída. Enfim, sua principal característica era a ausência de um controle central.¹⁸⁸

Sob a influência de Licklider, e devido a inúmeros problemas de compatibilidade¹⁸⁹, os pesquisadores do IPTO passam a se debruçar na construção de um protocolo universal que permitisse que redes e dispositivos de diversas naturezas se comunicassem sem a necessidade de intervenção humana. Não obstante, era necessário desenvolver uma arquitetura descentralizada e aberta, que fosse o flexível o suficiente para permitir o início de um processo autônomo de desenvolvimento.¹⁹⁰ Após um ano de trabalho, o pesquisador Vint Cerf e seu grupo de pesquisas em Stanford concretizam a ideia que resultou no Transmission Control Protocol/Internet Protocol (TCP/IP):

Vint Cerf e seu grupo de pesquisas em Stanford trabalharam durante um ano para concretizar a ideia que resultaria no Transmission Control Protocol/Internet Protocol (TCP/IP): um conjunto de protocolos de comunicação em que o TCP cuidaria da transmissão de dados e da correção de erros, e o IP, do endereçamento. Os computadores de uma rede poderiam comunicar-se entre si e possibilitariam a evolução

¹⁸⁷ LOVELUCK, *op. cit.*, p. 50.

¹⁸⁸ *Ibid.*, p. 52.

¹⁸⁹ É imprescindível compreender que, nesse período, houve o desenvolvimento de inúmeras redes comerciais e não-comerciais, ou seja, não houve uma evolução linear de uma única rede, o que dificultou a interoperabilidade entre todas essas iniciativas. (*Ibid.*, p. 54).

¹⁹⁰ Esse conceito é também fundamental para compreender a natureza da rede mundial de computadores. Ela não foi desenhada para uma única aplicação, mas para ser uma infraestrutura geral onde poderiam ser desenvolvidas várias novas aplicações e serviços. Cf.: ARAYA; VIDOTTI, *op. cit.*, p. 26.

da rede como um sistema aberto de comunicação por computadores capaz de abranger o mundo inteiro (Castells, 2003, p.14-21).¹⁹¹

Portanto, o protocolo TCP/IP tem como objetivo gerenciar o recorte das informações em pacotes e sua reconstituição (TCP) e o endereçamento das máquinas para circulação dos referidos pacotes (IP). Essa divisão em duas camadas permitiu estabelecer uma separação entre uma função de processamento dos recortes (TCP) e o seu transporte (IP), fazendo com que não haja a necessidade de nenhum elemento dessa rede ter de conhecer a localização dos transmissores, receptores ou mesmo a natureza da mensagem transmitida:

O TCP/IP estabelecem a conexão física das infraestruturas materiais (cabos, fibra ótica, etc) e a camada aplicada dos serviços aos usuários (email, apps, www, etc). Isso garante que os pacotes de dados serão todos transportados da mesma forma, independentemente de seus remetentes, de seus destinatários e de seu conteúdo final. Eles permitem cada jogador agir sem preocupar-se com a ação de outros, pois a rede é desprovida de um centro, sendo incapaz teoricamente de limitar, condicionar ou filtrar o uso que é feito desse sistema.¹⁹²

Em 1974 é publicado por Vinton Cerf e Robert Kahn o artigo *A protocol for packet network interconnection*, que descreve o funcionamento da arquitetura de rede baseada no TCP/IP, que acaba se tornando o padrão de comunicação entre computadores nos Estados Unidos em 1980¹⁹³ e que acabou por ser utilizada como protocolo padrão da ARPANET cerca de nove anos depois da publicação do artigo.¹⁹⁴ Em 1975, a ARPANET é transferida para a *Defense Communication Agency* (DCA), passando a ser utilizada com fins militares. Isso gera um desconforto entre os pesquisadores que utilizam a rede para fins acadêmicos, até que em 1983 a rede passa a ser dividida em *Milnet* (Military Net), para uso militar, e Arpa-Internet, dedicada exclusivamente à pesquisa. A ARPANET permanece *online* até o ano de 1990, quando encerra suas atividades, dando lugar a uma série de acordos comerciais e colaborativos entre redes privadas que culmina em sua “privatização”:

A rede das redes que se formou durante a década de 1980 chamava-se ARPA-Internet, depois passou a se chamar-se Internet, ainda sustentada pelo Departamento de Defesa e operada pela National

¹⁹¹ ARAYA; VIDOTTI, *op. cit.*, p. 23.

¹⁹² LOVELUCK, *op. cit.*, p. 55.

¹⁹³ CASTELLS, *op. cit.*, p. 103.

¹⁹⁴ ARAYA; VIDOTTI, *op. cit.*, p. 23.

Science Foundation. Tendo-se tornado tecnologicamente obsoleta depois de mais de vinte anos de serviços, a Arpanet encerrou suas atividades em 28 de fevereiro de 1990. Em seguida, a NSFNET, operada pela National Science Foundation, assumiu o posto de espinha dorsal da Internet. Contudo as pressões comerciais, o crescimento de redes de empresas privadas e de redes cooperativas sem fins lucrativos levaram ao encerramento dessa última espinha dorsal operada pelo governo em abril de 1995, renunciando a privatização total da Internet, quando inúmeras ramificações comerciais das redes regionais da NSF uniram forças para formas acordos colaborativos entre redes privadas.¹⁹⁵

Após esse processo que culminou em sua privatização, a Internet não contava com qualquer autoridade de supervisão. Foi quando foram improvisadas várias instituições e mecanismos foram criados durante o desenvolvimento da Internet para que estes assumissem algum grau de responsabilidade pela gestão técnica da rede, além dos contratos de corretagem de atribuição de endereços da Internet.¹⁹⁶ Em verdade, esse ambiente relativamente autônomo de desenvolvimento reflete os valores de igualdade, autonomia individual e auto-organização descentralizada que influenciou diversos representantes, universidades e terceirizados que fizeram parte do desenvolvimento dos protocolos da ARPANET desde o ano de 1969.¹⁹⁷

Esse movimento fez com que a Internet se difundisse sem qualquer órgão regulador, até que em 1992 fosse outorgada à *Internet Society* a responsabilidade pela sua regulação. Posteriormente, em 1998, é criada a IANA/ICANN, mas a Internet continuava a ser um terreno sem nenhuma autoridade clara, tanto nos Estados Unidos como no mundo.¹⁹⁸

Por fim, Loveluck resume o advento da Internet descrevendo quatro características fundamentais para sua criação: 1) ela foi fruto de uma cooperação entre especialistas, mesmo que a distância, que deu origem a um grupo de pesquisadores que compartilhavam interesses de pesquisa em comum; 2) tratava-se de uma comunidade de iguais em que não existia uma autoridade clara, fazendo com que as discussões, avaliações e circulação de informações

¹⁹⁵ CASTELLS, *op. cit.*, p. 102.

¹⁹⁶ *ibid.*, p. 102.

¹⁹⁷ Esse grupo compunha o Network Working Group (NWG), implementado desde 1969 para definir os protocolos da ARPANET por meio de reuniões e documentos técnicos chamados de Request For Comments (RFC), que eram submetidos a grupos expandidos para discutir as decisões do NWG em formar consensos. Embora de forma mais formal, isso ocorre até hoje, sendo um elemento central da concepção da internet e sua ligação com ideais liberais de autorregulação. Cf.: LOVELUCK, *op. cit.*, p. 58.

¹⁹⁸ CASTELLS, *op. cit.*, p. 102.

por meio dos RFC's¹⁹⁹ fossem os protagonistas desse processo; 3) a colaboração e trabalho em equipe para que fosse possível resolver os incontáveis problemas de compatibilidade entre os computadores e; 4) a criação de um mundo à parte, com regras particulares feitas especialmente para essa comunidade de especialistas em informática e pesquisadores. Essa junção de características acabou por deixar uma marca ainda muito presente na Internet atualmente, caracterizada como uma “forma de liberalismo pelos protocolos técnicos e pelos procedimentos destinados a instituir tais protocolos, organizando as interações da forma mais eficaz possível, mas de forma menos hierárquica possível, para que se desenvolva a autonomia dos indivíduos”.²⁰⁰

Em paralelo aos movimentos de tentativa de regulação da Internet, um novo salto tecnológico permite a aceleração da difusão da Internet na sociedade como um todo – a criação da Web, ou o WWW (*World Wide Web*). Essa aplicação foi desenvolvida para organizar a informação, conteúdos e sítios da Internet por um endereço amigável, e não por uma mera localização numérica:

A Web é um espaço de informação abstrato (imaginário). Na Internet você encontra computadores – na Web, você encontra documentos, sons vídeos, informação. Na Internet, as conexões são cabos entre computadores; na Web, as conexões são os links de hipertextos. A Web existe devido a programas que se comunicam entre computadores na Internet. A Web não poderia ser criada sem a Internet. A Web se tornou a rede útil porque as pessoas estão realmente interessadas em informação (para não citar conhecimento e sabedoria!) e realmente não querem saber sobre computadores e cabos.²⁰¹

A arquitetura do WWW é proposta em março de 1989 por Berners-Lee e Robert Cailliau, pesquisadores do *European Organization for Nuclear Research* (CERN), tendo como propósito inicial gerir e transferir informações pela Internet utilizando um sistema de navegação por links – o hipertexto. O objetivo era ajudar os pesquisadores do CERN a compartilhar informações do laboratório permitindo que os usuários navegassem facilmente em páginas utilizando links:

Em outubro de 1990, Berners-Lee criou um programa navegador/editor que permitia a criação e a edição de páginas de hipertexto, bem como a navegação por elas. O programa recebeu o nome de World Wide Web. Para a efetivação dessa tecnologia, Berners Lee precisou criar: a linguagem de etiquetas de hipertexto HTML (Hyper Text Markup

¹⁹⁹ “Request for Comments”.

²⁰⁰ LOVELUCK, *op. cit.*, p. 59.

²⁰¹ ARAYA; VIDOTTI, *op. cit.*, p. 26.

Language) para possibilitar a realização de páginas Web que todos os computadores do mundo pudessem exibir de maneira idêntica; o protocolo HTTP (Hyper Text Transfer Protocol), um jogo de regras que os computadores usariam para comunicar-se na Internet e permitiria links para recuperar automaticamente documentos, independentemente de sua localização; e o URL (Uniform Resource Locator), uma forma-padrão de dar aos documentos na Internet um único endereço. Em seguida, juntou tudo na forma de um servidor Web que armazenaria documentos HTML e os disponibilizaria para outros computadores fazendo solicitações HTTP para documentos com URLs. Em dezembro desse ano, Berners-Lee já havia desenvolvido todas as ferramentas necessárias para fazer a Web funcionar: o primeiro navegador, o primeiro servidor Web e as primeiras páginas Web (Sherman & Price, 2001, p.10-11).²⁰²

Esse contexto evolucionar que culmina no advento da Internet e, como visto, da Web, permite, segundo Castells, a criação da lógica de funcionamento de redes.²⁰³ É a partir desse marco tecnológico que diversas aplicações e tecnologias baseadas na rede mundial de computadores passam a ser desenvolvidas. Desde os primeiros buscadores, plataformas colaborativas, *streaming* de áudio e vídeo, redes e mídias sociais, armazenamento em nuvem, enfim, a economia movida a dados passa, antes de qualquer coisa, pela criação da Internet. A partir disso, diversas outras tecnologias passam a fazer uso das possibilidades criadas por essa rede. Do *Big Data* às técnicas de Inteligência Artificial, novas revoluções surgem, e, com isso, novos riscos.

2.2. O *BIG DATA* COMO NOVO MARCO TECNOLÓGICO: HIPERCONECTIVIDADE E TRATAMENTO DE DADOS

Dados, sozinhos, tem pouca utilidade humana. São elementos sem qualquer interpretação ou finalidade para que algum conhecimento seja gerado. Apesar disso, dados são coletados, armazenados e processados desde os primeiros indivíduos, conforme sempre houve um desejo de apurar a compreensão sobre o meio ambiente para empregar decisões melhores.²⁰⁴ Conforme analisado no capítulo anterior, a Internet transformou o modo de comunicação, transferência e armazenamento de informações. Desde então – e

²⁰² *ibid.*, p. 28.

²⁰³ CASTELLS, *op. cit.*, p. 107.

²⁰⁴ FORGÓ, N., HÄNOLD, S., SCHÜTZE, B. The Principle of Purpose Limitation and Big Data. In: Corrales, M., Fenwick, M., Forgó, N. (eds) *New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation*, Springer, Singapore, 2017. p. 18. ISBN 978-981-10-7055-5.

ela foi fundamental para a consolidação desse processo - o volume de dados utilizados para as mais diversas finalidades de tratamento passou a crescer de forma exponencial, especialmente após o crescimento no número de dispositivos que podem ser conectados à rede mundial de computadores.

Embora o *Big Data* tenha um conceito totalmente diferente da Internet, é fato que esta tornou muito mais fácil a coleta e o compartilhamento de dados. Todavia, enquanto a Internet é um meio de comunicação revolucionário, o *Big Data* vai além, permitindo aprender coisas ao analisar imensos conjuntos de dados, antes impossíveis de serem relacionados sem a tecnologia necessária.²⁰⁵

Hoje, não são só os computadores que se conectam à Internet. Dispositivos dos mais variados tipos estão conectados com a capacidade de coletar, analisar, armazenar e compartilhar dados. Esse é o conceito de Internet das coisas (IoT – *Internet of Things*), por exemplo.²⁰⁶ Há uma infinidade de equipamentos com essa capacidade, como os *smartphones*, os *wearables*²⁰⁷, carros autônomos, assistentes virtuais como a Alexa, Siri e Bixby. Até cafeteiras, máquinas de lavar, robôs aspiradores de pó e geladeiras podem estar conectados à rede mundial de computadores. Seus sensores, dos mais diversos tipos, geram dados que são utilizados com diversas finalidades – seja por seus próprios consumidores ou pelas organizações com algum interesse nas valiosas informações geradas por esses equipamentos. Estima-se que em 2021, 79 *zettabytes* de dados tenham sido criados, capturados, copiados ou consumidos no mundo. Esse número corresponde a impressionantes 79 trilhões de *gigabytes*. A estimativa é que em 2025 esse número alcance o volume de 181 *zettabytes*.²⁰⁸

Para conceituar o *Big Data*, é imprescindível compreender a sua natureza de processamento de dados ainda brutos, obtidos de diferentes fontes e relacionados de tal forma que gerem *insights*, auxiliando o ser humano em alguma tomada de decisão, ou mesmo para obter alguma informação antes

²⁰⁵ CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. The Rise of Big Data: How It's Changing the Way We Think About the World. **Foreign Affairs**, v. 92, n. 3, p. 28-40, 2013. p. 28. Disponível em: <http://www.jstor.org/stable/23526834>. Acesso em: 12 dez. 2022.

²⁰⁶ MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. p. 22.

²⁰⁷ Dispositivos pessoais que coletam dados em nosso corpo em tempo real.

²⁰⁸ TAYLOR, Petroc. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. In: **Technology & Telecommunications**, 2022. Disponível em: <https://www.statista.com/statistics/871513/worldwide-data-created/>. Acesso em: 02 fev. 2023.

desconhecida.²⁰⁹ Tal característica de análise de grandes conjuntos de dados brutos permite, por meio de processadores avançados, algoritmos inteligentes, softwares inovadores e matemática estatística, resultados nunca vistos em termos de processamento e geração de informação extraída de dados:

Em vez de tentar "ensinar" um computador a fazer coisas, como dirigir um carro ou traduzir entre idiomas, o que os especialistas em inteligência artificial tentaram fazer sem sucesso por décadas, a nova abordagem é inserir dados suficientes em um computador para que ele possa inferir a probabilidade de que, digamos, um semáforo seja verde e não vermelho [...] Usar grandes volumes de informações dessa maneira requer três mudanças profundas na forma como abordamos os dados. A primeira é coletar e usar uma grande quantidade de dados, em vez de se contentar com pequenas quantidades ou amostras, como os estatísticos fazem há mais de um século. A segunda é abandonar nossa preferência por dados altamente selecionados e imaculados e, em vez disso, aceitar a confusão: em um número crescente de situações, um pouco de imprecisão pode ser tolerado, porque os benefícios de usar muito mais dados de qualidade variável superam os custos de usar quantidades menores de dados muito exatos. Em terceiro lugar, em muitos casos, precisaremos desistir de nossa busca para descobrir a causa das coisas, em troca de aceitar correlações. Com Big Data, em vez de tentar entender com precisão por que um motor quebra ou por que o efeito colateral de um medicamento desaparece, os pesquisadores podem coletar e analisar grandes quantidades de informações sobre esses eventos e tudo o que está associado a eles, procurando padrões que possam ajudar a prever ocorrências futuras. Big Data ajuda a responder o que, não por que, e muitas vezes isso é bom o suficiente.²¹⁰

Trata-se, portanto, para além de uma nova tecnologia, de uma mudança de abordagem por parte dos cientistas de dados, uma transformação na forma como a sociedade processa as informações, deixando de tentar compreender as razões do porquê algo acontece para identificar as correlações entre os dados por meio do *Big Data*. O "como" deixa de ser o foco principal de análise, passando a ser a associação entre os fenômenos analisados o grande produto dessa tecnologia.²¹¹

São diversos os autores que se propuseram à tarefa de tentar conceituar esse fenômeno. Há, todavia, alguns traços em comum em relação a praticamente todas as proposições de definição. O conceito de *Big Data* é sempre relacionado com um grande conjunto de dados que são muito complexos

²⁰⁹ Não por acaso, os conceitos de Internet das Coisas e Big Data estejam de alguma maneira relacionados. Conforme mais coisas são conectadas à Internet, mais dados brutos são disponibilizados para algum tipo de análise e processamento posterior. Cf.: MAGRANI, *op. cit.* 2018, p. 22.

²¹⁰ CUKIER; MAYER-SCHOENBERGER, *op. cit.*, p.29

²¹¹ CUKIER; MAYER-SCHOENBERGER, *op. cit.*, p.32

e volumosos para serem processados por sistemas e metodologias de análise tradicionais. É o caso, por exemplo, de um projeto de mobilidade urbana na Estônia que utiliza uma série de dados dos seus cidadãos para melhorar o planejamento do transporte público do país.²¹² Para que isso ocorra, é necessário que haja a coleta de diversos tipos de dados dos cidadãos em grandes volumes e velocidade para que estes sejam relacionados de forma a permitir que haja informações precisas, ricas e rápidas para permitir a tomada de decisão dos gestores públicos responsáveis pela mobilidade urbana no país. Esse tipo de processamento só é possível com o uso de *Big Data*, ou seja, a aplicação deve ser capaz de processar uma quantidade gigantesca de dados de várias fontes diferentes e em um período muito curto de tempo.²¹³

Nesse sentido, o *Big Data* não pode ser considerado um sistema inteligente *per se*, mas sim uma metodologia que permite que computadores possam processar e organizar dados para deduzir a recorrência de eventos, independentemente de eles estarem previamente estruturados para o seu tratamento.²¹⁴

O exemplo do projeto de mobilidade urbana da Estônia ajuda a compreender o conceito inicialmente desenvolvido por Laney, que propõe uma perspectiva tridimensional do *Big Data* – conhecida como os 03 (três) “v’s” do *Big Data*. Essa perspectiva descreve determinadas características de uma aplicação que utilize *Big Data* deve ter. São elas: volume, variedade e velocidade. Em relação à primeira característica, esta muitas vezes é confundida com o próprio conceito de *Big Data* – é necessário um cenário com uma grande quantidade de dados sendo processada. Variedade, por sua vez, se relaciona com diferentes fontes e tipos de dados. Isso eleva o grau de complexidade de processamento dessas informações uma vez que elas normalmente não seguem um padrão que facilite sua compreensão. Ou seja, a aplicação *Big Data* deve ser capaz de processar e relacionar dados como imagens, textos, planilhas,

²¹² ESPON. Using big data for policy-making in the public interest. In: **ESPON BLOG**, 2020. Disponível em: <https://www.espon.eu/using-big-data-policy-making-public-interest>. Acesso em: 15 nov. 2022.

²¹³ CAPP, F.; FRANCO, S.; ROSSO, F. Citizens and cities: Leveraging citizen science and bigdata for sustainable urban development. **Business Strategy and the Environment**, v. 31, n. 2, p. 648–667, 2022. p. 652.

²¹⁴ BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 1. ed. Rio de Janeiro: Forense, 2018. p. 41.

sensores, estejam eles estruturados ou não.²¹⁵ A aplicação deve ser capaz de relacioná-los sem necessidade de intervenção humana. Por fim, outra característica fundamental é a velocidade em que os dados são transmitidos e processados. No exemplo já mencionado da Estônia, percebe-se os 03 (três) “v’s” em ação: há coleta e tratamento de uma grande quantidade de dados dos cidadãos (volume) com os mais variados tipos de dados como localização de dispositivos móveis, informações demográficas e imagens de satélite (variedade), além da capacidade do sistema gerar *insights* para tomada de decisão em tempo real (velocidade). Complementarmente, alguns autores acrescentam outras características ao *Big Data*, sugerindo a adição de mais 03 (três) “v’s”: veracidade, visualização e valor. A veracidade pode ser descrita como um atributo ligado à qualidade dos dados, sua confiabilidade para que seja de fato útil na obtenção de resultados. Quanto à característica da visualização, ela se relaciona com a sua utilidade em extrair dados e a capacidade de tomar decisões preditivas. Finalmente, a característica de valor se relaciona com a possibilidade de gerar valor econômico com base nas informações extraídas pelo conjunto de dados em *Big Data*.²¹⁶

Forgó, Hanold e Shutze também estabelecem três fases do *Big Data*. A primeira delas, denominada de fase de aquisição de dados, é o processo pelo qual os dados são filtrados ou selecionados antes de serem armazenados pelos sistemas capazes de processá-los. A origem desses dados são diversas como os já mencionados dispositivos *IoT*, ou os coletados em redes sociais, *smartphones* e *wearables*. Na segunda fase, os dados são mesclados e relacionados para gerar novos *insights* para extrair informações relevantes para alguma tomada de decisão. Por fim, a terceira fase consiste no uso dos resultados gerados pelo *Big Data*. Esta última é a fase mais importante, vez que

²¹⁵ Dados estruturados podem ser definidos como aqueles que são facilmente organizados, armazenados e transferidos por um modelo de dados definido, como, por exemplo, tabelas relacionadas de uma planilha, como nome, data de nascimento, CPF, entre outros. Dados não estruturados, por sua vez, são aqueles que não são facilmente acessados ou analisados pelos computadores de maneira automática. Podem ser conteúdos complexos como imagens, vídeos, postagens. Ou seja, eles não apresentam qualquer estrutura lógica previamente definida que permita relacioná-los com outros dados. Cf.: BOFF, Salette Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de Dados e Privacidade: Do direito às novas tecnologias na Sociedade Informacional**. Rio de Janeiro: Lúmen, 2018. p. 205)

²¹⁶ OLIVERA, Dânton Hilário Zanetti de. **Big Data e os limites à livre iniciativa no âmbito da Lei geral de proteção de dados pessoais**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Paraná, PPGD, 2022. p. 48.

será, de fato, o momento em que diversas aplicações serão realizadas com as informações extraídas durante o processo.²¹⁷

A utilização do *Big Data* envolve, deste modo, uma infinidade de questões computacionais. A análise preditiva, por exemplo, é uma abordagem muito utilizada para obter informações e padrões sobre os dados para que seja possível criar modelos preditivos, ou seja, analisar os dados do passado para obter informações em tempo real e prever eventos futuros.²¹⁸ Quanto maior a base e a variedade de dados, melhor e mais fidedignos serão os resultados previstos. Esse tipo de processamento de dados se baseia em técnicas de aprendizagem de máquina (*machine learning*), uma tecnologia que constrói a si própria e que pode ser personalizada e aplicada para executar uma vasta gama de tarefas preditivas. Nesse sentido, a aprendizagem de máquina permite lidar com questões desconhecidas, baseando-se num processo de aprendizado com uma grande base de dados. Trata-se, portanto, de um método de reconhecimento de padrões de forma autônoma e sem interferência humana, que utiliza uma fórmula numérica chamada de modelo estatístico probabilístico.²¹⁹

Cynthia Freitas e Jean Paul Barddal explicam que as tarefas de predição também são tecnicamente conhecidas como “generalização”, tratando-se de a capacidade de um modelo preditivo extrair o comportamento dos dados, permitindo prever com precisão os dados ainda desconhecidos. Tais técnicas de aprendizagem de máquina podem ser divididas em modelos preditivos de classificação ou regressão:

A classificação é uma tarefa em que um modelo preditivo é construído para distinguir objetos de diferentes classes, dadas suas características (features). A partir de um conjunto de um conjunto de dados contendo os recursos que descrevem objetos e suas classes, um modelo preditivo pode ser construído. Após sua construção, o modelo pode ser consultado para prever a categoria de um objeto, dadas suas características. [...]

Em contraste com a classificação, a tarefa de regressão tem o objetivo de aprender um modelo que prediz um valor contínuo, em lugar de um valor discreto. Supondo as aplicações mencionadas anteriormente, a

²¹⁷ FORGÓ, HÄNOLD, SCHÜTZE, *op. cit.*, 2017. p. 20.

²¹⁸ FREITAS, Cynthia Obladen de Almendra; BARDDAL, Jean Paul. Análise preditiva e decisões judiciais: controvérsia ou realidade? **Democracia Digital e Governo Eletrônico**, v. 1, p.107-126, 2019. p. 110.

²¹⁹ OLIVEIRA, Carla. Aprendizado de máquina e modulação do comportamento humano. In: **Sociedade de Controle: Manipulação e modulação nas redes digitais**. 1. ed. São Paulo: Hedra, 2018. p. 75.

previsão do mercado de ações e as previsões meteorológicas (temperatura e precipitação) são tarefas típicas aos modelos de regressão. Nesses problemas, o objetivo é prever um valor contínuo (valor do estoque, temperatura ou precipitação das chuvas), esperando minimizar a diferença entre o valor real e as previsões.²²⁰

Embora não se confunda com o conceito de Inteligência Artificial (IA)²²¹, o *machine learning*, conforme estudado, pode ser considerado um ramo de IA que se baseia na capacidade de um sistema de "aprender", ser treinado, a partir de exemplos, sem que seja explícito um conjunto de regras para seguir, a partir da análise de conjuntos de dados.²²²

Em suma, a inteligência artificial é uma área da informática que se preocupa com a criação de sistemas capazes de realizar tarefas que normalmente exigiriam inteligência humana, como reconhecimento de padrões, aprendizado, planejamento e resolução de problemas. Tanto a IA quanto o *Big Data* são tecnologias dependentes do vultoso aumento de dispositivos conectados na Internet que coletam e transmitem, por meio de crescentes espécies de sensores, os mais variados tipos de dados. Estima-se que em 2030, mais de 29 bilhões de dispositivos estarão conectados na Internet²²³,

²²⁰ Cinthia Freitas e Jean Paul Barddal elencam ainda uma terceira divisão, chamada de tarefa de agrupamento ou *clustering*. Trata-se de uma tarefa descritiva, utilizada para entender o comportamento subjacente que existe nos dados, como por exemplo, a segmentação de fluxos de cliques que representam as atividades de um usuário na web. ANÁLISE PREDITIVA E DECISÕES JUDICIAIS: controvérsia ou realidade? Cf.: FREITAS; BARDDAL, *op. cit.*, p. 111.

²²¹ Os primeiros estudos sobre IA datam de 1942, com o artigo "A *logical calculus of the ideias immant in nervous activity*", escrito pelo psiquiatra Warren S. Mcculloch e pelo cientista cognitivo Walter Pitts. O artigo faz analogias entre o funcionamento das células nervosas de nosso cérebro e processos eletrônicos. O termo "inteligência artificial" foi cunhado pela primeira vez em 1956 na Conferência de Dartmouth, na qual um grupo de cientistas da computação, incluindo John McCarthy e Marvin Minsky, se reuniram para discutir a possibilidade de criar máquinas que poderiam pensar e aprender como humanos. Desde então, várias pesquisas sobre o tema vêm sendo desenvolvidas. Durante as décadas de 1950 e 60, a pesquisa de IA concentrou-se em tentar criar máquinas que pudessem realizar tarefas específicas, como jogar xadrez ou resolver equações matemáticas. Esse tipo de IA é projetado para executar uma tarefa específica em vez de ser uma inteligência geral. Nas décadas de 1970 e 1980, a pesquisa de IA começou a migrar para a criação de "sistemas especialistas", que foram projetados para replicar as habilidades de tomada de decisão de um especialista humano em um domínio específico. Foi a partir dos anos 90 e início dos anos 2000 que a IA passa a ser amplamente utilizada em uma variedade de aplicações com o avanço em tecnologias de aprendizagem de máquina, processamento de linguagem natural e inteligência artificial baseada em regras, que permitiram a criação de assistentes pessoais virtuais, sistemas de reconhecimento de fala e veículos autônomos. Cf.: OLIVEIRA, *op. cit.*, p. 75.

²²² OLIVEIRA, *op. cit.*, p. 75.

²²³ VAILSHERY, Lionel Sujay. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. In: **Technology & Telecommunications**, 2022. Disponível em: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>. Acesso em: 02 fev. 2023.

alimentando uma indústria bilionária que visa explorar tais informações para as mais diversas finalidades.

2.3. CONSEQUÊNCIAS DA HIPERCONNECTIVIDADE PARA A CRIAÇÃO DE RISCOS DA SOCIEDADE INFORMACIONAL

A hiperconectividade que decorre do aumento da utilização de tecnologias, que fazem uso da Internet, como por exemplo as ferramentas que realizam tratamento de dados fazendo uso do *Big Data*, traz novos desafios aos legisladores de políticas públicas e ao direito. É crucial que haja um debate sobre como a utilização de dados pessoais para o tratamento, compartilhamento e, especialmente, a monetização desses ativos impactam o desenvolvimento dos indivíduos e da própria sociedade.

As tecnologias analisadas, embora tragam indiscutíveis benefícios à sociedade, quando utilizadas sem qualquer controle podem ser aplicadas para modular o comportamento humano, bem como suscitar inúmeras preocupações em relação ao direito à privacidade. Se esse novo mundo orientado a dados é inevitável, com máquinas tomando decisões baseadas em algoritmos e a diminuição da fronteira entre o ser humano e a máquina, é essencial compreender as questões éticas e os riscos que decorrem desse novo estágio da humanidade. A decisão sobre que tipo de mundo deve ser concebido daqui para frente deve ser consciente, com amplo debate público e com medidas de balanceamento de direitos e de mitigação de risco.

Se em sua concepção a Internet tinha uma proposta democratizante e descentralizadora do poder, hoje ela assume características muito diferentes. Atualmente, pouquíssimas organizações concentram um poder, provavelmente nunca visto na história, dominando o desenvolvimento de tecnologia e processamento de dados em um local muito bem definido – o vale do silício. Estima-se que Apple, Microsoft, Meta (empresa controladora do Facebook, Whatsapp e Instagram), Alphabet (empresa controladora do Google) e Amazon tenham, somadas, valor de mercado superior a 6 (seis) trilhões de dólares.²²⁴

²²⁴ LARICCHIA, Federica. Leading tech companies worldwide 2022, by market capitalization. In: **Technology & Telecommunications**, 2023. Disponível em:

Para efeito comparativo, a soma de todas as riquezas produzidas (PIB) pelo Japão é inferior a esse valor, e ele só perde para China e Estados Unidos no ranking dos países com maior economia mundial.²²⁵

Evgeny Morozov, pesquisador bielorrusso das implicações sociais e políticas do progresso tecnológico e digital, é um ferrenho crítico dessa concentração de poder. O autor afirma que o modelo capitalista centrado em dados adotado pelo vale do silício transforma todos os aspectos da existência humana em um ativo extremamente rentável para as *big techs*²²⁶, termo dado para as grandes empresas de tecnologia que dominam o mercado de tecnologia no mundo²²⁷. Não só isso, ainda segundo o autor, tais tecnologias, exportadas para todo o mundo e utilizadas por bilhões de pessoas, refletem as ideologias norte-americanas, deixando pouco espaço para que os usuários de plataformas e mídias sociais tenham contato com outras visões de mundo:²²⁸

Vivemos num momento em que nossas risadas num show de comédia são contabilizadas e analisadas em conjunto com os livros que compramos, os sites que visitamos, as viagens que fizemos, as calorias que consumimos. Tudo é integrado num perfil específico que pode ser monetizado e aperfeiçoado. Assim, as rupturas são viabilizadas pelas crises políticas e econômicas, não pela tecnologia. E elas nos afetam profundamente na forma como vivemos e nos relacionamos: é muito difícil preservar valores como a solidariedade num ambiente tecnológico que prospera com base na personalização e experiências únicas e individuais.²²⁹

O pesquisador, nesse sentido, não responsabiliza a tecnologia em si pelas crises do século XXI, mas sim a dominação de um dos mais preciosos ativos da atualidade – a informação – por um pequeno conjunto de empresas concentradas em uma região da Califórnia que, orientadas por um capitalismo

<https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/>. Acesso em: 02 fev. 2023.

²²⁵ DIMITROPOULOU, Alexandra. Economy Rankings: Largest countries by GDP, 2022. In: **CeoWorld Magazine**, 2022. Disponível em: <https://ceoworld.biz/2022/03/31/economy-rankings-largest-countries-by-gdp-2022/#:~:text=World%20GDP%3A%20The%20World%27s%20GDP,countries%20from%202019%20to%202026>. Acesso em: 21 out. 2022.

²²⁶ MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política**. Tradução Cláudio Marcondes. São Paulo: UBU Editora, 2018. p. 33.

²²⁷ Outro termo comumente utilizado para descrever grandes empresas de tecnologia é GAFAM, acrônimo de 5 das maiores empresas de tecnologia do mundo: Google, Apple, Facebook, Amazon e Microsoft. (FONTANEL, Jacques. GAFAM, a progress and a danger for civilization. Financial Architecture; **Forced Economic Development ion the Context of External Shocks and Internal Inconsistencies**, St. Peters-burg State University of Economics (UNECON), Apr 2019, Saint-Petersbourg, Russia. hal-02102188)

²²⁸ *ibid.*, p. 15.

²²⁹ *ibid.*, p. 47.

neoliberal, trabalham incessantemente em ferramentas e serviços que em nada contribuem ativamente para a redução das desigualdades sociais e mazelas da sociedade, embora enriqueçam os seus fundadores e acionistas.²³⁰

Stefano Rodotá, pesquisador italiano que estudou os impactos da sociedade da vigilância na privacidade, também relaciona a concentração de poder em grandes organizações e suas consequências sociais:

Essa é uma interrogação central, visto que a substancial reserva da infra-estrutura informativa para os sujeitos privilegiados, públicos ou privados que seja, tem uma consequência óbvia: a de aumentar as possibilidades de discriminação e os desníveis de poder no interior de uma organização social.²³¹

A grande mudança ocorrida na Sociedade Informacional nas duas últimas décadas foi a popularização das plataformas e mídias sociais desenvolvidas por essas empresas onde o usuário, além de um consumidor de conteúdo, é frequentemente estimulado a produzi-lo.²³² Vive-se, nesse sentido uma nova era do capitalismo, caracterizando um novo sistema econômico que possui como base de sua concepção a utilização de técnicas de *data mining* e *profiling*.²³³

Segundo Shoshana Zuboff, trata-se de “uma nova forma de capitalismo informacional que visa prever e modificar o comportamento humano como forma de produzir receita e controle de mercado”.²³⁴ Nesse sentido, aqueles que dotam dos meios de modificação de comportamento, como as plataformas digitais e mídias sociais, concentram uma forma de poder equivalente ou até superior à propriedade dos meios de produção, conforme analisado no capítulo 1.1.

²³⁰ *ibid.*, p. 51.

²³¹ RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 40.

²³² MACHADO, 2018a, *op. cit.*, p. 48.

²³³ *Data Mining* ou mineração de dados é o processo de descobrir padrões em grandes conjuntos de dados envolvendo métodos na interseção de aprendizado de máquina, estatísticas e sistemas de banco de dados. É um campo interdisciplinar que se baseia em técnicas de áreas como ciência da computação, estatística e ciência da informação. O *profiling* ou perfilamento, por sua vez, refere-se ao processo de coleta e análise de dados sobre um determinado indivíduo ou grupo, a fim de entender suas características, hábitos e preferências. Isso pode ser usado para uma variedade de finalidades, como marketing, pesquisa ou segurança. A criação de perfis pode envolver técnicas de mineração de dados, mas também pode envolver outros métodos de coleta e análise de dados. Cf.: HAN, Jiawei; PEI, Jian; KAMBER, Micheline. *Data Mining. The Morgan Kaufmann Series in Data Management Systems*. Saint Louis: Elsevier Science & Technology, 2011

²³⁴ ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2020. p. 75.

Há inúmeros autores que trabalham a modificação do comportamento humano por meio das plataformas digitais com o propósito de servir à expansão do neoliberalismo. Embora o desenvolvimento tecnológico seja essencial para a evolução da sociedade, entender esse fenômeno é importante para compreender de que forma o direito à privacidade é impactado por essas tecnologias, além de construir soluções para combater eventuais abusos, traçando limites do que é ou não aceitável em relação à utilização de dados pessoais pelas organizações públicas e privadas.

Atualmente, o desenvolvimento das plataformas digitais faz uso, entre outros métodos, de algoritmos capazes de aprimorar sua capacidade de tratar dados pessoais e analisar o nosso comportamento por meio de técnicas que fazem uso do *Big Data* e *machine learning*. Tais tecnologias podem, a depender do contexto e aplicação, filtrar nossa comunicação e nos inserir em bolhas de pessoas semelhantes, o que acarreta inúmeros riscos ao livre desenvolvimento da personalidade.²³⁵

Stefano Rodotá, ao analisar os impactos da sociedade da vigilância na privacidade, afirma que a criação de filtros automatizados:

[...] Podem ocasionar a discriminação das pessoas que não correspondem ao modelo geral, acentuando a estigmatização dos comportamentos desviantes e a penalização das minorias. Pode-se identificar aqui um obstáculo ao pleno desenvolvimento da personalidade individual, cerceada em meio a perfis historicamente determinados. Ao se privilegiar de comportamentos conformes aos perfis predominantes, torna-se difícil a criação de novas identidades coletivas, com riscos para a própria dinâmica social e para a organização democrática. Diante disso, deve ser vigorosamente assegurado o "direito de deixar rastros" sem receber por isso nenhuma penalidade.²³⁶

Esse obstáculo ao desenvolvimento, conforme mencionado pelo autor, ofende diversos fundamentos e princípios legais do ordenamento jurídico brasileiro, seja na esfera constitucional ou infraconstitucional. A LGPD, por exemplo, prevê como objetivo e fundamento da Lei o livre desenvolvimento da personalidade, bem como oferece ao titular de dados pessoais²³⁷ o direito de solicitar a revisão de eventuais decisões tomadas em processos automatizados

²³⁵ SILVEIRA, *op. cit.*, p. 34.

²³⁶ RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008 p. 104.

²³⁷ Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. (Art. 5, V, LGPD)

que afetem, entre outras questões, aspectos ligados à sua personalidade. Não obstante, embora não haja menção expressa a esse direito na CRFB, a doutrina é uníssona ao afirmar que se trata de um direito fundamental garantido pela Carta Magna brasileira, vez que ela protege amplos direitos sociais, econômicos, culturais e ambientais.²³⁸

Também se dá, nesse sentido, a projeção da proteção à personalidade por meio dos dados pessoais. Segundo Anderson Schreiber, os direitos da personalidade se relacionam com “atributos humanos que exigem especial proteção no campo das relações privadas, ou seja, na interação entre particulares, sem embargo de encontrarem fundamento constitucional e proteção nos planos nacional e internacional”.²³⁹ Nesse sentido, os direitos da personalidade podem ser considerados todos como o conjunto de qualidades incorpóreas e corpóreas que fazem parte da projeção da pessoa humana, estando incluídos nesse conceito a proteção ao nome, honra, integridade física e psíquica, privacidade, entre outros.²⁴⁰ Se há, nesse sentido, atividades de processamento de dados que, de alguma forma, toca essa projeção da pessoa humana, há de se justificar “dogmaticamente a inserção dos dados pessoais na categoria dos direitos da personalidade, assegurando, por exemplo, que uma pessoa exija a retificação dos seus dados pessoais para que a sua projeção seja precisa.”²⁴¹

A modulação do comportamento também pode ocorrer conforme algoritmos utilizam amplas bases de dados (*Big Data*) para prever e induzir indivíduos a comportamentos para as mais diversas finalidades, mas notadamente em função da retenção da atenção e influência em decisões de compra de consumidores.²⁴² Esses algoritmos estão presentes em quase todas

²³⁸ Nesse sentido, há diversos estudos que elencam o direito ao livre desenvolvimento da personalidade como categoria de direitos fundamentais previstos pela CRFB. Tal afirmação ocorre por uma interpretação integrativa da Constituição, em que se reconhece um direito geral da personalidade decorrente de uma compreensão histórica de lutas pela realização da dignidade humana. Cf.: DE MARCO, Cristhian Magnus; DE CASTRO, Matheus Felipe. As dimensões e perspectivas do direito fundamental ao livre desenvolvimento da personalidade. **Revista Prisma Jurídico**, v. 12, n. 1, 2013. Disponível em: <https://periodicos.uninove.br/prisma/article/view/4253/2530>. Acesso em: 12 dez. 2022.

²³⁹ SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas. 2014, p. 13.

²⁴⁰ BIONI, *op. cit.*, p. 63

²⁴¹ *ibid.*, p. 65.

²⁴² CASSINO, João Francisco. Modulação deleuziana, modulação algorítmica e manipulação midiática. In: **Sociedade de Controle: Manipulação e modulação nas redes digitais**. 1. ed. São Paulo, SP. Hedra, 2018.p. 27.

as ações realizadas *online*, como nos mecanismos de pesquisa que ajudam a encontrar sites, notícias e documentos, nos anúncios veiculados na Internet, nas postagens e *feeds* de redes sociais. Enfim, são os algoritmos que permitem o processamento de forma massiva e automatizada de dados, sendo essenciais para o modelo de negócio dos serviços e plataformas *online*.²⁴³

Nesse sentido, há uma economia baseada em vigilância, conforme observa Bruno Bioni:

Uma economia que tem como cerne a vigilância. É a observação permanente do comportamento dos indivíduos que a movimenta, sendo as suas informações pessoais a matéria-prima a ser explorada para a geração de riqueza. Mais do que isso, há um “varejo de dados pessoais”. Par a operacionalização desse modelo de negócio, há uma complexa rede de atores que transaciona as informações pessoais dos consumidores, agindo cooperativamente para agregar mais e mais dados e, em última análise, tornar a mensagem publicitária ainda mais eficiente.²⁴⁴

Um dos principais aspectos que permeiam os algoritmos são a forma como eles afetam diretamente a percepção de mundo dos indivíduos que utilizam serviços e plataformas na Internet. Embora muitas vezes eles sejam desenvolvidos de forma objetiva e neutra, raramente eles se mantêm completamente imunes de interferências culturais dos seus criadores.²⁴⁵ Não só a programação dos algoritmos está sujeita a isso, mas as próprias bases de dados utilizadas para o processo de aprendizagem de máquina são potencialmente tendenciosas, vez que reflete escolhas e decisões humanas. Ou seja, elas podem apresentar preconceitos, também chamados de “vieses”.²⁴⁶

Nesse sentido, e por serem projetados com fins econômicos, os algoritmos desenvolvidos no contexto das plataformas e serviços *online* normalmente visam incentivar comportamentos e estruturar preferências de forma a identificar e classificar pessoas.²⁴⁷ As grandes empresas de tecnologia, por exemplo, projetam produtos que deliberadamente estimulam ansiedades – como o ato de atualizar constantemente os *feeds* no Instagram e Twitter.²⁴⁸

²⁴³ MACHADO, 2018a, *op. cit.*, p. 49.

²⁴⁴ BIONI, *op. cit.*, p. 49.

²⁴⁵ MACHADO, 2018a, *op. cit.*, p. 50.

²⁴⁶ FREITAS; BARDDAL, *op. cit.*, p. 120.

²⁴⁷ MACHADO, 2018a, *op. cit.*, p. 50.

²⁴⁸ MOROZOV, *op. cit.*, p. 29.

Essa engenharia psicológica, que conta com as mentes mais brilhantes do planeta trabalhando constantemente nesses projetos, servem aos interesses econômicos das maiores empresas de tecnologia do mundo, restando pouca ou nenhuma atenção para os efeitos e riscos que isso gera à sociedade. Não se trata de depreciar a tecnologia, mas sim de haver uma conduta crítica em relação ao modo como ela vem sendo utilizada para mercantilizar e explorar economicamente cada aspecto da vida humana, desde as questões mais íntimas, até as nossas conexões e relacionamentos digitais.²⁴⁹

Nesse sentido, a modulação do comportamento humano pode se dar de diversas formas. A mais comum delas ocorre por meio do processo de controle da visualização de conteúdo. Esse processo se difere para cada plataforma, pois cada uma conta com sua própria arquitetura de informação. Ao controlar as opções e caminhos de interação e acesso ao conteúdo, as plataformas e mídias sociais organizam a visualização de conteúdo de forma extrair o maior tempo e atenção possível dos usuários. Além disso, toda a arquitetura deve ser concebida para que os usuários se sintam bem, confortáveis e acessíveis a eventuais anúncios que apareçam em sua *timeline*.²⁵⁰

Ainda que haja um esforço do usuário em não expor certas informações sobre sua vida, há uma infinidade de rastros digitais deixados nas mais corriqueiras tarefas do dia a dia. Esses dados podem ser utilizados para melhorar produtos e serviços, mas, também, serem utilizados para modular e influenciar as pessoas.²⁵¹ É o caso, por exemplo, das ferramentas de aprendizado de máquina utilizado pela Meta (Facebook, Instagram e Whatsapp) que filtram os anúncios, postagens e notícias do *feed* de suas mídias sociais:

O usuário tem a ilusão de que escolhe o que lê, visualiza, curte, compartilha, comenta, mas isso é uma falsa liberdade. Na verdade, quem classifica, exclui e decide o que aparece na timeline é um algoritmo de aprendizado de máquina. Esse tipo de algoritmo destrói a capacidade do ser humano de escolher outros mundos possíveis ou que poderiam vir a existir. Ou seja, limita a visão de mundo das pessoas.²⁵²

²⁴⁹ MOROZOV, *op cit.*, p. 30.

²⁵⁰ SILVEIRA, *op. cit.*, p. 38.

²⁵¹ OLIVEIRA, *op. cit.*, p.86.

²⁵² OLIVEIRA, *op. cit.*, p. 93.

Essa modulação por meio de algoritmos que induzem comportamentos compõe um dos elementos centrais do que alguns autores chamam de sociedade de controle, que nasce no final do século XX e início do XXI, conforme ocorrem os avanços das tecnologias de comunicação em massa e, mais recentemente, as tecnologias digitais em rede.²⁵³ Essa sociedade de controle se difere da sociedade disciplinar, que, por sua vez, é caracterizada, pela sua função de docilizar comportamentos por meio do poder aplicado sobre os corpos. A sociedade disciplinar está temporalmente vinculada à revolução industrial, momento em que houve a necessidade de criar instituições disciplinares para fiscalizar o ser humano que se concentrava cada vez mais nos centros urbanos, além do surgimento da figura do operário.²⁵⁴

Assim, se na sociedade disciplinar o ser humano seguia sua vida com base no medo da punição pelas instituições (tais como a escola, o hospital, o presídio), hoje os instrumentos de modulação de condutas trabalham subjetivamente tocando a personalidade das pessoas por meio do afeto, da melhora da experiência, do estímulo criativo. Trata-se de uma espécie de “liberdade controlada”.²⁵⁵

O filósofo coreano Byung-Chul Han dá o nome a esse contexto de “regime da informação”, caracterizado pela forma de dominação com a qual a informação aliada a técnicas de tratamento de dados por algoritmos e IA, determinam decisivamente em processos sociais, políticos e econômicos:

Em oposição ao regime disciplinar, não são corpos e energia que são explorados, mas informações e dados. Não é então a posse dos meios de produção que confere poder, mas o acesso a dados utilizados para vigilância, controle e prognóstico de comportamentos psicopolíticos. O regime de informação está acoplado ao capitalismo da informação, que se desenvolve em capitalismo de vigilância e degrada seres humanos em gado, em animais de consumo e dados.²⁵⁶

Nesse sentido, não se fala mais de uma forma de vigilância centralizada, mas de uma sociedade transparente, onde todos vigiam todos. Ainda segundo o

²⁵³ CASSINO, *op. cit.*, p. 14.

²⁵⁴ CASSINO, *op. cit.*, p. 15.

²⁵⁵ MACHADO, 2018a, *op. cit.*, p. 58.

²⁵⁶ Ainda segundo o autor, no capitalismo da informação as técnicas disciplinares se tornam obsoletas. O sujeito submetido ao regime da informação é livre e criativo. A comunicação é fortemente explorada e o regime de vigilância é explorado por meio dos dados. Cf.: HAN, Byung-Chul. **Infocracia**: Digitalização e a crise da democracia. 1. ed. Petrópolis: Editora Vozes, 2022. p. 7.

autor, os habitantes desse novo “panóptico digital”²⁵⁷ imaginam estar em liberdade, quando na verdade não estão. O que assegura a transparência dessa sociedade é justamente a hiperconectividade ou, nas palavras do filósofo, da “hipercomunicação”.²⁵⁸ A sociedade de controle, portanto, se consoma no momento em que os sujeitos dessa sociedade, ao imaginarem estar em liberdade, colaboram ativamente para a manutenção desse sistema sem necessidade de coação externa, mas a partir de uma vontade interna. Assim, “o medo de renunciar à sua esfera privada e íntima dá lugar à necessidade de se expor à vista sem qualquer pudor”.²⁵⁹

A sociedade de controle é marcada pelo uso das TICs para “modular, cristalizar uma determinada subjetividade desejada na memória, no cérebro das pessoas”.²⁶⁰ Trata-se, portanto, da atuação sutil e ubíqua que atua nos cérebros e influencia as pessoas em suas escolhas, modulando o seu comportamento para, entre outros objetivos, capturar o máximo possível de sua atenção. O filósofo francês Gilles Deleuze desenvolveu o conceito de modulação, conhecido como “modulação deleuzeana”, que pode ocorrer, entre outras formas, pela modulação algorítmica. Segundo o filósofo, esse tipo de modulação é subsidiado por enormes bancos de dados, induzindo comportamentos e influenciando na retenção de atenção e decisões de compras dos indivíduos.²⁶¹

Não obstante, as grandes empresas de tecnologia se esforçam para criar experiências e espaços de “liberdade”, mas, ao supervisionarem todos os aspectos da nossa existência por meio de algoritmos cuidadosamente criados para captar a nossa atenção, acabam por adotar formas panópticas de vigilância.²⁶² Dessa forma, o estímulo para a hipercomunicação e hiperinformação por meio da hiperconectividade não gera, necessariamente, mais verdade e bem-estar. Mais informação significa, também, mais pobreza de atenção. Logo, cria-se uma nova economia – a da escassez de atenção.²⁶³ E para apreender a atenção do consumidor, algoritmos o categorizam para ofertar

²⁵⁷ HAN, Byung-Chul. **Sociedade da transparência**. 1. ed. Petrópolis: Editora Vozes, 2016. p. 107.

²⁵⁸ *ibid.*, p. 108.

²⁵⁹ *ibid.*, p. 109.

²⁶⁰ CASSINO, *op. cit.*, p. 15.

²⁶¹ CASSINO, *op. cit.*, p. 22.

²⁶² HAN, 2016, *op. cit.*, p. 116.

²⁶³ CASSINO, *op. cit.*, p. 18;

mundos personalizados de consumo, informação, trabalho e lazer. Esses mundos não são reais, mas são extremamente eficientes para a captação da atenção e venda de anúncios personalizados.²⁶⁴

O valor econômico da Sociedade Informacional, que é transparente e direcionada ao controle, está concentrada na quantidade e velocidade de troca de informações, e não na obtenção de mais bem-estar e mais verdade.²⁶⁵ É nisso que reside um dos grandes riscos da Sociedade Informacional – o estímulo econômico flui sem considerar todas as consequências negativas da hiperconectividade, geradas pelas TICs, aqui entendidas como as restrições ao livre desenvolvimento da personalidade e aos direitos à privacidade. Não há discussão de que são incontáveis os benefícios dessas tecnologias, mas há um excesso de exposição que visa transformar tudo em mercadoria mediante uma coação indireta por transparência e uniformização.²⁶⁶ Assim, se você não se expõe, você não existe.

Nisso reside uma crítica fundamental a respeito da adoção de novas tecnologias pela sociedade – há um constante debate sobre como as ferramentas digitais podem ser úteis ou não ao ser humano, mas há uma carência de um debate público sobre como essas tecnologias viabilizam ou inviabilizam sistemas sociais, políticos e econômicos.²⁶⁷

Reverter esse processo de modulação do comportamento pelas *Big Techs* parece uma missão impossível. O acúmulo de poder, tamanho e popularização são tão grandes que qualquer esforço nesse sentido está fadado ao fracasso. Resta tentar implementar medidas de controle, gestão de risco e regulações que tragam algum equilíbrio a essa relação.

2.4. PRIVACIDADE E TRATAMENTO DE DADOS PESSOAIS NA SOCIEDADE HIPERCONNECTADA

Como visto, a Sociedade Informacional hiperconectada gera, ao contrário do que se possa presumir e apesar da grande quantidade de informações que a

²⁶⁴ CASSINO, *op. cit.*, p. 28.

²⁶⁵ HAN, 2016, *op. cit.*, p. 25.

²⁶⁶ HAN, 2016, *op. cit.*, p. 35.

²⁶⁷ MOROZOV, *op. cit.*, p. 41.

caracterizam, uma carência de verdade a partir do momento em que as escolhas humanas passam a ser modularizadas pelas TICs. Há cada vez mais coleta, tratamento e difusão de informações que condicionam diretamente o modelo de organização política, social e econômica, impactando diretamente nos riscos criados pela Sociedade Informacional.²⁶⁸ Nesse sentido, Han afirma que “mais informação e mais comunicação não afastam a fundamental falta de precisão do todo. Pelo contrário, intensifica-a ainda mais”.²⁶⁹

É nesse contexto que surge o debate sobre como o direito à privacidade responde à utilização das TICs para o tratamento de dados pessoais em escalas cada vez maiores. Há quem diga, nesse sentido, que a privacidade como direito se tornou uma mercadoria de alto valor agregado, ou seja, ela deixou de ser algo que desfrutamos gratuitamente para ser um valioso produto. Privacidade seria algo caro e, portanto, para poucos²⁷⁰, o que remete, inclusive, ao seu nascimento ligado às conquistas e privilégios da classe burguesa e as transformações socioeconômicas relacionadas à revolução industrial.²⁷¹

Há, todavia, um extenso e importante debate sobre como a privacidade vêm se transformando enquanto ocorre o avanço do uso das TICs pelo poder público e privado. Atribuir à privacidade uma mera proteção à esfera privada é verdadeiramente insuficiente em vista das inúmeras consequências individuais e coletivas geradas pelo tratamento de dados no contexto da Sociedade Informacional. O debate da modulação algorítmica, da sociedade de controle e da formação dos filtros bolha, conforme analisado no último capítulo, é essencial para compreender que é preciso analisar a privacidade para além do “direito a ser deixado só”²⁷², mas também na esfera da organização do poder e da infraestrutura da informação que lhe dá significado.²⁷³

Nesse sentido, um dos principais pontos que caracterizam os paradigmas da Sociedade Informacional é a progressiva substituição dos bens materiais pelos serviços culturais no cerne da produção social. Assim, a defesa da

²⁶⁸ RODOTÁ, *op cit.*, p. 63.

²⁶⁹ HAN, 2016, *op. cit.*, p. 25.

²⁷⁰ RODOTÁ, *op cit.*, p. 36.

²⁷¹ Nesse sentido, o nascimento de um direito à privacidade no contexto das lutas da classe burguesa remete a um vínculo desse direito à própria noção de propriedade. Cf.: RODOTÁ *op cit.*, p. 27.

²⁷² WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, p. 193-220, dez. 1890.

²⁷³ RODOTÁ, *op cit.*, p. 24.

personalidade assume um papel fundamental para que haja alguma proteção para o tratamento de dados pessoais nos mais diversos contextos, sejam eles públicos ou privados. Para Alain Touraine, esse deslocamento do material para o cultural também gera a substituição da ideia de luta de classes da sociedade industrial para um contexto de defesa da personalidade contra a lógica dos aparatos e mercados que dominam a produção e disseminação de informações no século XXI.²⁷⁴

Se há um novo contexto social, há, também, a necessidade de atribuir um novo significado ao direito à privacidade, escapando do seu significado tradicional de mera proteção à intimidade. Stefano Rodotà trabalha esse processo evolutivo da privacidade:

[...] parece cada vez mais frágil a definição de “privacidade” como o “direito a ser deixado só”, que decai em prol de definições cujo centro de gravidade é representado pela possibilidade de cada um controlar o uso das informações que lhe dizem respeito. [...] hoje chama a atenção sobretudo para a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados na disponibilização de informações, concorrendo assim para estabelecer equilíbrios sócio-políticos mais adequados”.²⁷⁵

Nesse sentido, as TICs corroboram, especialmente num contexto generalizado de tratamento de dados pessoais com diversas finalidades, para essa evolução do conceito da privacidade, que passa a estar ligado mais à possibilidade do seu titular de “conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas”.²⁷⁶ Não obstante, essa tendência se traduz numa progressiva ampliação da esfera privada, passando a compreender não somente a intimidade do indivíduo, mas também todo o conjunto de ações, comportamentos, opiniões, enfim, tudo aquilo que possa ocasionar alguma forma de controle ou gerar estigma social em relação ao seu titular. Portanto, as TICs, ao corroborarem para a hiperconectividade, expõem o ser humano a diversas ameaças, o que exige, em contrapartida, a necessidade de um progressivo fortalecimento da proteção jurídica da privacidade:²⁷⁷ “Foi a presença de riscos conexos ao uso de informações coletadas (e não uma vocação natural ao sigilo) que fez com que houvesse um reconhecimento ao

²⁷⁴ CASTELLS, *op. cit.*, p. 78.

²⁷⁵ RODOTÁ, *op. cit.*, p. 24.

²⁷⁶ RODOTÁ, *op. cit.*, p. 92.

²⁷⁷ RODOTÁ, *op. cit.*, p. 95.

‘direito à autodeterminação informativa’ como um direito fundamental do cidadão.”²⁷⁸

Trata-se, portanto, da construção de um direito à privacidade que seja capaz de conferir um verdadeiro poder de controle ao indivíduo, não somente a uma eventual interrupção do tratamento ou eliminação dos seus dados, mas de exigir formas de “circulação controlada” e uso legítimo dos seus dados pessoais.²⁷⁹

Essa legitimidade está ligada diretamente ao princípio da finalidade do tratamento de dados e consiste numa das principais fontes de discussão sobre o tratamento de dados pessoais que se utilizam do *Big Data*. O princípio da finalidade é previsto pelo art. 6º, inciso I da LGPD, que conta com a seguinte redação:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.²⁸⁰

Nesse sentido, tal princípio passa a ser fundamental para que o tratamento de dados pessoais que segue sua coleta seja considerado legítimo, no sentido que só poderão ser realizados os tratamentos necessários à realização dos propósitos informados ao titular. O contexto do *Big Data* é especialmente desafiador justamente por suas características de permitir a relação de diversas bases de dados sem contar com finalidades previamente definidas, conforme explica Dânton Zanetti:

A problemática recebe contornos ainda mais complexos quando relacionada à realidade do *Big Data*, haja vista que, por sua natureza, o *Big Data* não necessariamente conta com finalidades previamente definidas. Isto porque, tanto o uso agregado de dados, como sua reutilização em diferentes contextos e para diversas finalidades, muitas delas futuras e sequer imagináveis ao tempo da coleta dos dados, são da própria essência do *Big Data*.²⁸¹

²⁷⁸ *ibid.*, p. 96.

²⁷⁹ *ibid.*, p. 93.

²⁸⁰ BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022..

²⁸¹ OLIVEIRA, 2022, *op. cit.*, p. 56.

Não obstante, dada a relação assimétrica existente entre os titulares de dados e as organizações que realizam tratamento de dados pessoais, tampouco o consentimento se revela suficiente para legitimar toda e qualquer operação de tratamento com dados pessoais em que o titular haja consentido. Este é, na acepção jurídica do termo, (hiper)vulnerável em relação ao mercado informacional, nas palavras de Bruno Bioni:

Nesse sentido, as diversas oportunidades na sociedade atual estão condicionadas ao fornecimento dos dados pessoais. Cada vez mais, a participação social é dependente desse trânsito informacional. Na verdade, a lógica do mercado e da Sociedade Informacional arquitetam essa (falsa) escolha, já que, para fazer parte do jogo, deve-se aceitar o convite mediante o “concordo” em compartilhar os “meus” dados pessoais. Daí por que a proteção de dados pessoais geraria um custo social, qual seja, a não fruição dessas oportunidades que resultaria em uma eremitania na Sociedade Informacional.²⁸²

Não obstante, Stefano Rodotà também entende pela insuficiência do consentimento, especialmente pois ele reduziria a privacidade a valores puramente proprietários e mercadológicos, sem qualquer preocupação com as consequências sociais de determinadas categorias de tratamento de dados pessoais:

Daí se deduz a impossibilidade de fazer operar o consentimento em todos os casos: e isto significa também a impossibilidade de fundar no consentimento a definição de privacidade. Além disso, não se podendo considerar todos os dados como livremente negociáveis, limita-se a possibilidade de recorrer à lógica de mercado.²⁸³

Nesse sentido, os usuários não estão preparados, nem em relação à compreensão das consequências, nem pela dificuldade de dar plena transparência do alcance do consentimento como ferramenta de controle do fluxo de dados pessoais.²⁸⁴

Embora pareça – e seja – essencial conferir controle sobre a circulação de dados pessoais, há inúmeras pressões econômicas em sentido contrário. Segundo Carl Bildt, Presidente do Instituto de Pesquisa *Global Commission on Internet Governance*²⁸⁵, “as barreiras contra a livre circulação de dados são, na

²⁸² BIONI, 2019, *op. cit.*, p. 164.

²⁸³ RODOTÁ, *op. cit.*, p. 77.

²⁸⁴ LANA; D’ALMEIDA, *op. cit.*, p. 74.

²⁸⁵ Global Commission on Internet Governance. Disponível em: <https://ourinternet.org/>. Acesso em: 20 out. 2022.

verdade, barreiras contra o comércio”.²⁸⁶ Tal afirmação não poderia ser mais verdadeira. A circulação de dados internacionalmente é hoje um dos aspectos mais fundamentais do capitalismo informacional, sendo objetivo de diversos tratados internacionais para a viabilização dessa livre circulação de dados entre diversas nações.²⁸⁷

Em contrapartida, é justamente a pressão generalizada ocasionada pela necessidade de crescimento econômico do capitalismo informacional que gera eventuais abusos e utilização de dados pessoais para finalidades escusas e um tanto obscuras. De fato, o crescimento econômico, o comércio internacional e as liberdades civis são fundamentos da nossa sociedade para viabilizar o estado de bem-estar social. Todavia, há uma indissociabilidade entre o valor normativo do direito fundamental à privacidade como um dos pilares da democracia liberal, e nisso reside em grande parte a natureza política das tecnologias que realizam tratamento de dados pessoais.²⁸⁸

Nesse sentido, é fundamental considerar a privacidade como parte integrante do rol das dimensões mais elevadas de direitos civis e da democracia, vez que não é possível atribuir a ela uma lógica puramente proprietária, ou seja, um direito de natureza puramente individual que pode ser negociado em uma lógica contratual. Em suma, “não se pode efetivamente estimar que os interesses ligados à proteção de dados sejam de ordem inferior”.²⁸⁹ Tal concepção sobre o direito à privacidade encontra guarida na CRFB ao garantir a inviolabilidade da intimidade e da vida privada em seu art. 5º, inciso X, além dos artigos 11 e 21 do Código Civil (CC) e artigo 2º, inciso IV da LGPD.

2.5. CONTORNOS DA DIMENSÃO DIGITAL DA SOCIEDADE DE RISCO

A partir da análise realizada nos capítulos anteriores, se estabelecerão algumas relações entre os riscos criados a partir da Sociedade Informacional e

²⁸⁶ MOROZOV, *op. cit.*, p. 73.

²⁸⁷ São exemplos de tratados para a transferência internacional de dados: Tratado de Lisboa; Convenção 108 de 1981; Passenger Name Records (PNR); Terrorist Financing Tracking Programme (TFTP).

²⁸⁸ HENRIQUE NETO, Sylvio. **Democracia e tecnologia da informação**: o tríplice conflito entre criptografia, vigilância e privacidade nos Estados Unidos. 2019. Tese (Doutorado em Ciência Política) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2019. p. 99. Acesso em: 02 fev. 2023.

²⁸⁹ RODOTÁ, *op. cit.*, p. 53.

a ligação destes com as características que compõem a segunda modernidade descrita por Beck, em uma tentativa de configurar os contornos de uma eventual dimensão digital da Sociedade de Risco.

Conforme examinado no tópico 1.5, Ulrich Beck estabelece alguns elementos que configuram a Sociedade de Risco, caracterizada como uma fase da sociedade em que os riscos decorrentes do processo de modernização passam a ter determinadas características que fogem ao controle dos tradicionais mecanismos de proteção institucional da Sociedade Industrial. Nesse sentido, tais riscos são dotados de elevado nível de abstração e complexidade, culminando em uma ausência de “percepção, de previsibilidade e de controle em torno de situações fáticas que, criadas pelo momento da inovação, são experimentadas sem que haja uma efetiva consciência sobre o que se experimenta.”²⁹⁰

O primeiro elemento configurador da Sociedade de Risco é a relação entre risco, espaço e tempo. Tal elemento vincula-se ao fato de que, na primeira modernidade, os riscos encontravam-se limitados em função do tempo e de um espaço geográfico. São as evoluções tecnológicas que geram novos riscos e fenômenos que transcendem os limites temporais e espaciais até então estabelecidos. Nesse sentido, os riscos não podem mais ser contidos em espaços geográficos definidos, bem como seus possíveis impactos transcendem a atualidade, podendo impactar as gerações presentes e futuras.²⁹¹

Conforme analisado no presente trabalho, as tecnologias que envolvem as TICs podem assumir características pervasivas. A Internet, como meio de manifestação de diversos riscos, não respeita fronteiras ou espaços geográficos. Os riscos da utilização massiva de dados para as mais diversas finalidades, culminando em uma sociedade de vigilância por meio de tecnologias ubíquas, com inúmeras repercussões sociais, culturais e econômicas que escapam à percepção dos seus usuários, ainda são incertos, não sendo facilmente identificados no tempo e espaço.

²⁹⁰ FREITAS; Cinthia Obladen de Almendra; FERREIRA, Heline Sivini; CAVEDON, Ricardo. Reflexões sobre o direito à autodeterminação informacional a partir das bolhas informacionais e dos riscos associados aos mecanismos de busca diante da personalização do usuário de internet. In: NETO, José Querino Tavares; FREITAS, Cinthia Obladen de Almeida; COSTA, Andréa Abrahão. **Métodos e pesquisas avançadas em direito**. Curitiba: CRV, 2021. p. 43.

²⁹¹ FERREIRA, 2008, *op. cit.*, p. 40.

O subsequente elemento caracterizador da Sociedade de Risco é a falência dos padrões de segurança como consequência do processo acelerado de modernização. Esse colapso resulta na diminuição da proteção e no aumento dos riscos que não podem mais ser adequadamente controlados pelas instituições da sociedade industrial. Esse processo ocorre conforme nasce o conceito de irresponsabilidade organizada, que segundo Goldblatt, consiste em “um encadeamento de mecanismos culturais e institucionais pelos quais as elites políticas e económicas encobrem efectivamente as origens e consequências dos riscos [...] catastróficos da recente industrialização”.²⁹² Tais mecanismos são, segundo Heline Sivini Ferreira, o exercício simbólico da ciência, o uso simbólico da política e a função simbólica do direito.²⁹³

Segundo a autora, na segunda modernidade a ciência não se relaciona somente com a tecnologia, mas também com a indústria (aqui entendida como o conjunto de organizações privadas desenvolvedoras de tecnologias), fazendo com que seja impossível separar os conceitos de ciência, tecnologia e indústria. Isso faz com que a ciência se afaste cada vez mais de um ideal de certeza e controle, ou seja, das reais consequências de determinadas tecnologias.²⁹⁴ Nesse sentido, o exercício simbólico da ciência consiste, resumidamente, no ato de produzir cientificamente um conhecimento falso ou parcial, com o propósito de atender interesses específicos, evitando revelar a real natureza da ciência analisada.²⁹⁵ Nesse contexto, a construção de verdades figuradas é nociva ao público, na medida que ela pode ser utilizada para produzir desinformação por meio de conhecimentos simbólicos isentos de neutralidade e imparcialidade.²⁹⁶

O uso simbólico da política, por sua vez, consiste em utilizar a definição de metas e medidas anunciadas com o propósito escuso de alcançar resultados totalmente fictícios, tratando-se, em verdade, de uma estratégia política para dissimular a verdade e promover um falso estado de normalidade.²⁹⁷ Por fim, a função simbólica do direito é um mecanismo de reforço da irresponsabilidade

²⁹² GOLDBLATT, David. **Teoria social e ambiente**. Tradução Ana Maria André. Lisboa: Piaget, 1998. In: FERREIRA, Heline Sivini. **A biossegurança dos organismos transgênicos no direito ambiental brasileiro: uma análise fundamentada na teoria da sociedade de risco**. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina, CPGD, 2008. p. 52.

²⁹³ FERREIRA, 2008, *op. cit.*, p. 51.

²⁹⁴ FERREIRA, 2016, *op. cit.*, pp. 108-158.

²⁹⁵ FERREIRA, 2008, *op. cit.*, p. 55.

²⁹⁶ *ibid.*, p. 57.

²⁹⁷ *ibid.*, p. 58.

organizada, que ocorre quando normas são introduzidas no ordenamento jurídico sem qualquer efetividade prática, ou seja, não oferecem nenhuma proteção porque, ou estão cheias de lacunas, ou são ineficazes em regular a matéria que se propõem.²⁹⁸ Nessa perspectiva, esse parecia ser o panorama da proteção de dados pessoais no Brasil até a entrada em vigor da LGPD em 2020. Embora houvesse legislações setoriais que tratassem sobre a temática da proteção de dados, como o Código de Defesa do Consumidor (CDC), a Lei do Cadastro Positivo (LCP) e o Marco Civil da Internet (MCI), a falta de uma diretriz clara sobre as consequências de eventuais irregularidades (penalidades) e um arcabouço fiscalizatório (Autoridade Nacional de Proteção de Dados - ANPD) acabava por tornar as referidas legislações ineficientes na regulação da proteção de dados pessoais no Brasil. Nesse contexto, o grande desafio regulatório após a edição da LGPD se trata de dar efetividade à legislação, vez que cabe especialmente à ANPD definir os níveis de riscos aceitáveis ou toleráveis em relação ao tratamento de dados pessoais no Brasil. Sem essa adequada postura da autoridade, o avanço incondicional das TICs gera, como consequência, uma expansão irrestrita do desenvolvimento econômico, comprometendo um “processo regulamentar efetivamente funcional”.²⁹⁹

No contexto da Sociedade Informacional, são inúmeras as situações que se aproximam, em maior ou menor medida, do conceito de irresponsabilidade organizada descrito acima. Stefano Rodotá menciona a tendência, estimulada pelo mercado, de um “*derregulation*” em relação à temática da proteção de dados, estimulando a adoção de códigos de conduta, diretrizes setoriais, e outras formas de autorregulação que podem vir a ser utilizados de forma totalmente instrumental, ou seja, utilizando a tutela da privacidade como uma via para a legitimação social do uso de tecnologias que causam potenciais riscos à sociedade:

Em tal caso, a tutela da privacidade se apresenta como uma via para a legitimação social dessas tecnologias e, nesse sentido, pode incutir a suspeita de seu uso completamente instrumental. Ao mesmo tempo, porém, essa tendência alerta contra simplificações excessivas do problema das informações pessoais, porque é justamente nesse ponto que se localiza a fronteira entre a Sociedade Informacional e a sociedade da vigilância.³⁰⁰

²⁹⁸ *ibid.*, p. 60.

²⁹⁹ *ibid.*, p. 63.

³⁰⁰ RODOTÁ, *op cit.*, p. 126.

Na Sociedade Informacional, o uso simbólico da política, conforme descrito acima, sequer é necessário. Embora as pessoas se sintam livres, é o próprio sentimento de liberdade que assegura o controle da sociedade, que se faz quando liberdade e vigilância coincidem.³⁰¹ Âmbitos inconscientes são utilizados como formas de dominação, o *Big Data* e a IA exploram o inconsciente, oculto às pessoas impactadas pelas tecnologias. O regime da informação, nesse sentido, é capaz de influenciar o comportamento humano abaixo do limiar da consciência.³⁰²

Nesse ponto reside um risco crucial da Sociedade Informacional que se traveste em Sociedade de Risco – o regime da informação mina o processo democrático que tem como pressuposto a autonomia e a liberdade de vontade.³⁰³ Não faz parte dos objetivos do presente trabalho analisar as consequências da emergência da Sociedade de Risco na Sociedade Informacional em relação às suas consequências ao regime democrático, mas resta evidente que os riscos analisados neste estudo acentuam a crise da democracia.

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, imobilizando em torno de perfil historicamente determinados. E, em seu perfil sócio-político, ao privilegiar comportamentos "conformes", o controle pode tornar mais difícil a produção de novas identidades coletivas, reduzindo assim a capacidade total de inovação dentro do sistema. Em ambos os casos, o preço pago em termos de democracia é tudo menos irrelevante.³⁰⁴

O último elemento caracterizador da Sociedade de Risco é a noção de globalidade dos riscos, definido como a consequência de múltiplas crises que, embora independentes em relação à sua nacionalidade, são compartilhadas por toda a humanidade em diferentes níveis. Nesse sentido, a própria noção de Sociedade em Rede desenvolvida por Manuel Castells já corrobora para a presença dessa característica da Sociedade Informacional, especialmente com a Internet e sua pretensão de ser uma aldeia global. Os tratados e acordos sobre

³⁰¹ HAN, 2022, *op. cit.*, p. 16.

³⁰² HAN, 2022, *op. cit.*, p. 23.

³⁰³ HAN, 2022, *op. cit.*, p. 39

³⁰⁴ RODOTÁ, *op cit.*, p. 83.

livre circulação de dados como o *Trade In Services Agreement* (TISA), *Transatlantic Trade and Investment Partnership* (TTIP) e *Trans-Pacific Partnership* (TPP)³⁰⁵ visam todos promover a livre circulação de dados entre países, facilitando a utilização de dados para as mais diversas finalidades, entre elas a da modificação do comportamento humano que provoca crises sociais, econômicas e políticas, conforme já analisado.

As *Fake News*³⁰⁶, por exemplo, são uma clara consequência da Sociedade Informacional que impacta toda a humanidade, gerando uma crise de verdade que “prolifera-se onde desintegra a sociedade em tribos ou agrupamentos, não havendo mais possibilidade de conciliação”³⁰⁷. Nesse sentido, o processo de digitalização, que é global, enfraquece a consciência da realidade – perde-se a confiança nos fatos, transformado a Sociedade Informacional em uma Sociedade da Desconfiança.³⁰⁸

A própria consciência dos riscos abre um mundo paralelo que potencializa a desinformação. Há uma carência de uma distinção clara entre saber e não saber, entre o verdadeiro e falso, entre o bom e o mau. Na Sociedade de Risco, marcada pela irresponsabilidade organizada com a crise das instituições, conhecimento e desconhecimento se fundem para criar centenas de verdades sobre um risco – seja ele real ou potencial.³⁰⁹

Assim, dentre os riscos criados na modernidade avançada, conforme Beck denomina o estágio da humanidade em que se configura a Sociedade de Risco, somam-se aqueles decorrentes do emprego das TICs:

Dentre os riscos abstratos criados pela modernidade avançada, encontram-se aqueles decorrentes do emprego de novas tecnologias, a exemplo da informática. Ao possibilitar o armazenamento, a transmissão e o processamento de informações em meios digitais, a informática torna-se onipresente no cotidiano das pessoas, congregando uma variedade de riscos que não podem ser facilmente percebidos ou identificados.³¹⁰

³⁰⁵ MOROZOV, *op cit.*, p. 71.

³⁰⁶ Desinformação ou Fake News podem ser conceituadas como informações distorcidas, não filtradas, cujo propósito pode ser o de ludibriar ou manipular o público com implicações políticas e sociais. Cf.: PRIOR, H., *Mentira e política na era da pós-verdade: fake news, desinformação e factos alternativos*. In: LOPES, P.; REIS, B. (eds.) **Comunicação Digital: media, práticas e consumos** Lisboa: NIP-@M & UAL, pp. 75-97, 2019.

³⁰⁷ HAN, 2022, *op. cit.*, p. 83.

³⁰⁸ HAN, 2022, *op. cit.*, p. 94.

³⁰⁹ BECK, 2015, *op. cit.*, p. 24.

³¹⁰ CAVEDON; FERREIRA; FREITAS, *op. cit.*, p. 200.

Ainda segundo o autor, a Sociedade Industrial se transforma em uma Sociedade de Risco por meio dos seus próprios perigos de formas sistematicamente produzidas, prevalecendo uma racionalidade pautada na geração de oportunidades a partir de riscos e, com isso, ultrapassando o limite do que é seguro.³¹¹ Essa mesma racionalidade econômica é encontrada no modo como, contemporaneamente, se sujeitam os direitos da personalidade, especialmente o direito à privacidade, ao tratamento massivo de dados pessoais por organizações públicas e privadas:

Em razão do grande volume de dados pessoais que são constantemente compartilhados contemporaneamente - por meio de diversas redes - observa-se o desenvolvimento de uma Sociedade de Risco, na qual os indivíduos já não detêm o controle - nem do conteúdo e tampouco do acesso - das informações relacionadas a si mesmos.³¹²

O direito à privacidade deve ser compreendido, conforme analisado nos tópicos anteriores, em um sentido amplo, abarcando todas as esferas de manifestações da personalidade, ou seja, deve ser entendida como "o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito".³¹³

A criação de riscos na Sociedade Informacional por meio da hiperconectividade gera inúmeros efeitos coletivos. Os dados coletados do indivíduo, quando considerados em si mesmos, podem não ter significado ou qualquer potencial lesivo. No entanto, quando "se torna possível conhecer e relacionar toda a massa de informações relativas a uma determinada pessoa, do cruzamento dessas relações surge o perfil completo do sujeito considerado, que permite sua avaliação e seu controle por parte de quem dispõe do meio idôneo para efetuar tais operações".³¹⁴

A modernização descrita por Ulrich Beck se mostra, neste aspecto, perfeitamente aderente à noção de controle (ou a falta dele) ao direito à privacidade, trazendo à tona um turbilhão de novas e complexas situações

³¹¹ BECK, 2002, *op. cit.*

³¹² SPALER, Mayara Guibor; REIS, Rafael Almeida Oliveira. Limites do direito fundamental à privacidade frente a uma sociedade conectada. **Revista Jurídica da Escola Superior de Advocacia da OAB/PR**, Curitiba, v. 19, n. 31, p. 47-65, 2018.

³¹³ SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 26 ed. São Paulo: Malheiros, 2005. p. 206.

³¹⁴ RODOTÁ, *op cit.*, p. 61.

imprevisíveis e incontroláveis. Os efeitos negativos e as repercussões deste modelo de modernização inserem a Sociedade Informacional em um cenário de crise que necessita de uma adequada postura do Direito, devendo ser avaliado criticamente, tanto em relação a sua velocidade para dirimir os conflitos sociais oriundos da Sociedade da Risco, quanto a sua eficácia objetiva na prevenção dos riscos e efeitos negativos da crise das sociedades contemporâneas.³¹⁵

Atualmente, diante do impacto causado pelo avanço das TICs e suas aplicações hodiernas, bem como o alcance ilimitado em relação a circulação de dados pessoais em todo o mundo, é altamente complexo definir os limites do direito à privacidade em relação a necessidade do mercado de dados pessoais, bem como delimitar os riscos relacionados ao tratamento de dados pessoais em grande escala³¹⁶. Não raro, os indivíduos são impactados por decisões tomadas por modelos algoritmos e dados estatísticos, sendo estas informações a única representação dos indivíduos perante inúmeros agentes sociais – não só perante empresas privadas, mas também em relação a acesso a serviços públicos, como, por exemplo, no uso de TICs pelas *smartcities*³¹⁷.

Assim, é fundamental que haja uma reflexão sobre os impactos das TICs e a mudança de paradigma que transforma os dados pessoais em pura mercadoria. A própria dignidade da pessoa humana, ligada à proteção da personalidade, passa a ser secundária em relação aos interesses do mercado na livre circulação de dados. Segundo Stefano Rodotà, vivemos em uma época que inicia sua reflexão sobre as consequências sociais do uso das TICs. Em um interessante encontro de teorias, o autor italiano acaba por utilizar uma

³¹⁵ PINTO, Celciane Malcher. A sociedade de risco na visão de Ulrich Beck e suas conexões com o direito e meio ambiente. **Revista de Direito e Sustentabilidade**. Encontro Virtual, v. 7, n. 1, p. 73-91, Jan/Jul. 2021. e-ISSN: 2525-9687. p. 82.

³¹⁶ Mais do que isso, os dados pessoais passaram a ser objeto de grande preocupação nos últimos anos conforme cresceram o seu interesse comercial. Tais dados ganham novo significado a partir do incremento das tecnologias da informação e comunicação (TICs), que permitem a coleta, transferência e processamento de informações que podem vir a revelar novos aspectos da vida de uma pessoa. A manipulação de dados pessoais permite a criação de perfis individuais ou de um agrupamento de indivíduos, que podem ser utilizados para os mais diversos fins, tendo um valor inestimável ao mercado, que encaram os dados como “matéria-prima” essencial para o desenvolvimento de suas atividades e incremento dos seus resultados.

³¹⁷ Segundo a união europeia, *Smart Cities* são sistemas de pessoas interagindo e usando energia, materiais, serviços e financiamento para catalisar o desenvolvimento econômico e a melhoria da qualidade de vida. Esses fluxos de interação são considerados inteligentes por fazer uso estratégico de infraestrutura e serviços e de informação e comunicação com planejamento e gestão urbana para dar resposta às necessidades sociais e econômicas da sociedade. (<https://fgvprojetos.fgv.br/noticias/o-que-e-uma-cidade-inteligente>).

referência surpreendentemente relacionada à teoria da Sociedade de Risco de Ulrich Beck:

As TICs, até o momento, assumiram muito frequentemente características de tecnologias sujas, aproximando-se muito mais do modelo das tecnologias industriais poluentes, tornando-se fundamental, portanto, favorecer ou impor a introdução no ambiente informativo de tecnologias limpas.³¹⁸

Legislações de proteção de dados como a LGPD e o Regulamento Geral de Proteção de Dados (RGPD) europeu, estabelecem alguns mecanismos para o controle, pelo titular, dos seus dados pessoais, permitindo que os indivíduos possam – pelo menos de um modo geral, controlar o uso e disseminação de suas informações. Em relação às organizações que tratam os dados pessoais, as referidas legislações impõem uma série de requisitos e obrigações que aumentam na mesma proporção em que crescem os riscos oriundos da utilização dos dados.

Estabelece-se então, uma relação íntima entre o tratamento de dados pessoais e a gestão dos riscos inerentes ao seu uso, tema que é abordado no capítulo 3 (três) do presente trabalho, o qual apresenta uma análise do regime de proteção de dados pessoais no Brasil, bem como o papel da LGPD como marco regulatório brasileiro de proteção de dados.

Por fim, torna-se evidente que ambas as Sociedades (da Informação e de Risco) se relacionam de diversas maneiras. A primeira pode ser vista como um fator que contribui para a potencialização da segunda, conforme cresce a incerteza e vulnerabilidade na sociedade com o emprego das TICs e o seu potencial de ampliar as ameaças globais e criar, conforme analisado, riscos individuais, coletivos, sociais, econômicos e políticos.

³¹⁸ RODOTÁ, *op cit.*, p. 182.

3. REGIME DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL, FERRAMENTAS DE MITIGAÇÃO DE RISCO E A REGULAÇÃO POR ARQUITETURA

Os diversos riscos gerados pela tecnologia ao ser humano culminam em uma necessária resposta do Direito. Embora haja quem diga que regulações restritivas de coleta e tratamento de dados pessoais só sejam possíveis em tempos de tranquilidade social, é justamente em momentos de instabilidades políticas ou sociais em que há a necessidade de mais informações e ligação entre vários bancos de dados para enfrentar situações de emergência – como ocorreu, por exemplo, com a pandemia do COVID-19. São nesses momentos que se revela a indispensabilidade das legislações de proteção de dados para evitar o abuso de poder ou as distorções na utilização de dados pessoais dos cidadãos.³¹⁹

Para além das situações de excepcionalidade social, também houve, segundo Ulrich Beck, uma perda de controle dos perigos concebidos pela modernidade. Essa perda não foi necessariamente gerada por uma falha, mas justamente pelas vitórias do avanço da industrialização que, sistematicamente, desconsideraram as suas consequências para o ser humano e o meio ambiente.³²⁰ Nesse sentido, e conforme analisado em tópicos anteriores, a hiperconectividade assume um papel importante na geração desses riscos, caracterizado pelo aumento da interconexão e interdependência entre indivíduos, organizações e governos por meio de diversas tecnologias que fazem uso da Internet e do *Big Data*.

Consoante a análise feita no tópico 2.4, há um crescente debate sobre como a utilização das TICs geram riscos ao livre desenvolvimento da personalidade, notadamente à privacidade. Por sua vez, a tutela desse direito é fundamental para afirmação da dignidade da pessoa humana, tratando-se de um direito fundamental previsto pela Constituição. Assim, a defesa da personalidade humana assume uma característica de um direito geral, tutelando a

³¹⁹ RODOTÁ, *op cit.*, p. 51.

³²⁰ BECK, 2015, *op cit.*, p. 28.

personalidade humana em todas as suas manifestações para sua livre realização e desenvolvimento.³²¹

Isso implica em uma leitura não restritiva e taxativa dos direitos da personalidade, como, por exemplo, aqueles previstos pelo código civil brasileiro em seu capítulo II.³²² Estes não devem ser lidos de forma estanque, excluindo outras possibilidades de tutela da personalidade no ordenamento jurídico brasileiro, mas:

Sua leitura deve ser feita à luz da cláusula geral de proteção da personalidade presente na Constituição. A positivação no direito civil não é o que funda os direitos da personalidade, sua função é de orientar, interpretar e facilitar a aplicação e a tutela em hipóteses que a experiência e a natureza dos interesses fizeram com que o legislador fosse mais específico.³²³

Portanto, para além de um aspecto individual, a defesa da privacidade assume, segundo Danilo Doneda, um “elemento indutor de autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de

³²¹ DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2019. p. 91.

³²² Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Art. 12. Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau.

Art. 13. Salvo por exigência médica, é defeso o ato de disposição do próprio corpo, quando importar diminuição permanente da integridade física, ou contrariar os bons costumes.

Parágrafo único. O ato previsto neste artigo será admitido para fins de transplante, na forma estabelecida em lei especial.

Art. 14. É válida, com objetivo científico, ou altruístico, a disposição gratuita do próprio corpo, no todo ou em parte, para depois da morte.

Parágrafo único. O ato de disposição pode ser livremente revogado a qualquer tempo.

Art. 15. Ninguém pode ser constrangido a submeter-se, com risco de vida, a tratamento médico ou a intervenção cirúrgica.

Art. 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome.

Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.

Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.

Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.

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.

³²³ DONEDA, 2019, *op. cit.*, p. 96.

liberdade de uma forma geral”.³²⁴ A privacidade é, assim, pressuposta para a democracia, de modo que sua proteção garante, além da afirmação da dignidade da pessoa humana, o próprio estado democrático de direito.

Não obstante, a proteção constitucional desses aspectos individuais deve ser o fio condutor dos negócios jurídicos, de modo que o próprio direito privado deve se submeter à pessoa humana como categoria central de sua proteção.³²⁵ Assim, o indivíduo passa a ter uma proteção não somente em relação a atuação do Estado no que tange a privacidade e outros direitos humanos, mas, também, essa proteção passa a ser exercida principalmente perante os poderes privados, nos quais, hoje, encontra-se uma enorme concentração de poder em consequência da evolução tecnológica tratada nos capítulos anteriores.³²⁶

Compreender os contornos do direito à privacidade é, por fim, fundamental para que haja uma efetiva tutela da personalidade. O seu conceito passou por intensas ressignificações nas últimas décadas, conforme transformavam-se a noção de vida privada e o limite entre o público e privado.³²⁷

3.1. DA PRIVACIDADE AO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Em decorrência desse contínuo processo de evolução das TICs, hoje, a proteção da privacidade assume características muito diferentes da sua gênese. O desenvolvimento da sua definição passou por diversos caminhos, culminando em uma nova disciplina que passou a entender as garantias e princípios da privacidade em uma ótica mais abrangente, considerando outras formas de controle e repercussões para o indivíduo que se tornaram possíveis com o tratamento de dados pessoais por sistemas automatizados.³²⁸

As TICs passam a ter uma crescente importância nesse contexto, uma vez que as liberdades individuais são exercidas principalmente em estruturas ou

³²⁴ DONEDA, 2019, *op. cit.*, p. 131.

³²⁵ *ibid.*, p. 98.

³²⁶ *ibid.*, p. 97.

³²⁷ FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Privacidade e proteção de dados pessoais: perspectiva histórica. *InCID: Revista de Ciência da Informação e Documentação*, Ribeirão Preto, v. 12, n. 2, p. 151-172, set. 2021./fev. 2022.

³²⁸ *ibid.*, p. 177.

plataformas tecnológicas. Os problemas da privacidade foram ampliados, de forma que seu conteúdo passou a ser compreendido como “regras de circulação de informações”.³²⁹

Dessa forma, o tradicional “direito a ser deixado só”, conforme ocorreram os avanços das TICs e da Sociedade Informacional, passou por diversas redefinições, sendo entendido como o “direito de controlar o uso que os outros façam das informações que me digam respeito”, e, mais recentemente, como um “direito do indivíduo de escolher aquilo que está disposto a revelar aos outros”.³³⁰

As definições mais recentes revelam o modo como esse direito buscou tutelar aspectos ligados à personalidade humana conforme ocorrem os avanços tecnológicos. Atualmente, para Rodotá, a privacidade pode ser entendida como o “direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada”.³³¹ Nesse sentido, ainda segundo o autor, o objeto de proteção é um “patrimônio informativo atual ou potencial de um sujeito”.³³² Ou seja, a proteção da informação pessoal passa a ser o objetivo central do direito à privacidade:

Nesta definição, a informação (mais precisamente, as informações pessoais) coloca-se como elemento objetivo; e a construção da esfera privada, a finalidade, tomada em consideração juntamente com a cláusula geral da personalidade que a ressalta como um dos aspectos do livre desenvolvimento da personalidade.³³³

Assim, chega-se à conclusão de que, em decorrência do contexto tecnológico da Sociedade Informacional e das suas consequências (positivas e negativas) à pessoa humana, torna-se necessário que haja uma tutela mais dinâmica da privacidade, não se concentrando apenas no próprio sujeito de direito, mas que se possa proteger suas informações pessoais, ou seja, os dados que, de alguma forma, se desprendem da pessoa e passam a circular em suportes físicos e digitais.

Essas informações, embora eventualmente desvinculadas fisicamente do seu titular, mantém uma conexão intrínseca com a pessoa a quem se refere esses dados, representando-a diretamente. Assim, a informação pessoal (dado

³²⁹ RODOTÁ, *op cit.*, p. 63.

³³⁰ *ibid.*, p. 75.

³³¹ *ibid.*, p. 109.

³³² *ibid.*, p. 109.

³³³ DONEDA, 2019, *op cit.*, p. 135.

peçoal) de determinada pessoa a que se refere deve ser entendida como uma extensão da sua personalidade, e, portanto, estar sujeito a todas as implicações de direito aí decorrentes.³³⁴

Isto posto, a disciplina da proteção de dados pessoais passa a ser uma espécie de herdeira da disciplina da privacidade, preenchendo seu conteúdo com diversas formas de controle que se tornaram possíveis e necessárias com o aumento do tratamento de dados pessoais por organizações públicas e privadas.³³⁵

Foram vários os tipos de legislações que se preocuparam em regular a proteção de dados pessoais conforme ocorriam os avanços tecnológicos e sociais. Logo, é natural, sob esse aspecto, que existam as chamadas “gerações” de leis de proteção de dados pessoais. Se o modo como a sociedade lida com dados evoluiu, também a regulamentação sobre o seu uso deverá ser constantemente atualizada.

Atualmente, são quatro as gerações de legislações de proteção de dados identificadas pela doutrina, sendo que a primeira se inseriu num contexto em que enfatizava o controle por órgãos públicos de grandes bancos de dados estatais, evoluindo até a concepção atual, que elege o titular como principal protagonista das suas próprias informações, permitindo o controle sobre o seu uso por terceiros³³⁶. Ou seja, ela é caracterizada pela tentativa de, para além de uma tutela dos dados pessoais baseado na escolha individual, elevar o padrão coletivo de proteção de dados pessoais. Não obstante, as legislações de terceira e quarta geração colocam o risco das atividades de tratamento pelas organizações como um ponto de fundamental importância – qual seja – quanto maior o risco do tratamento, maiores deverão ser as precauções a serem

³³⁴ *ibid.*, p. 152.

³³⁵ *ibid.*, p. 178.

³³⁶ A segunda geração de leis de proteção de dados vai além do controle estatal dos bancos de dados, colocando o indivíduo como participante do processo decisório mediante o consentimento (autorizações). A terceira geração atingiu um conceito mais amplo de tutela ao direito à privacidade, ampliando a participação do indivíduo em todas as fases de uso dos dados pessoais, o que se chama de “autodeterminação informativa”. Por fim, a quarta e atual geração de legislações de proteção de dados contam com leis que priorizam o controle do titular sobre suas próprias informações, conforme explica Danilo Doneda: “Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção” (2006, p.98).

tomadas pelo controlador dos dados (suas obrigações de conformidade), bem como maior será a repercussão da responsabilidade em caso de incidentes.³³⁷

A lei brasileira de proteção de dados (LGPD) se encaixa nesses modelos, utilizando técnicas para fortalecer a posição dos indivíduos perante as organizações ou entidades que tratam dados pessoais, reconhecendo que há um natural desequilíbrio nessa relação, além de estabelecer regras de conformidade e controle de riscos pelas organizações públicas e privadas que tratam dados pessoais.³³⁸

Conquanto, passa-se a entender que algumas decisões não podem ser conferidas somente ao titular de dados pessoais, justamente por este não dotar de todas as informações necessárias para compreender os riscos relacionados ao tratamento de dados a que está sujeito, especialmente em algumas modalidades de tratamento que exigem um alto grau de proteção, como, por exemplo, no caso de dados pessoais sensíveis, de crianças ou adolescentes e os que geram perfis de consumo e hábitos do titular. A criação de autoridades independentes de proteção de dados também passa a ser a regra, justamente pela acentuação do desequilíbrio das relações entre os titulares e as organizações que tratam seus dados, havendo a necessidade de uma entidade que monitore e fiscalize as práticas do mercado em relação ao tratamento de dados pessoais.³³⁹

No Brasil, além da edição da LGPD que transforma toda a disciplina no ordenamento jurídico interno³⁴⁰, a Emenda Constitucional nº 115, de 10 de fevereiro de 2022, trouxe alterações à CRFB, incluindo a proteção de dados pessoais entre o rol de direitos e garantias fundamentais, além de fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. A primeira inclusão foi a do inciso LXXIX do art. 5º da Constituição Federal, que passou a vigorar com a seguinte redação: “é

³³⁷ LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito de Viçosa**, Viçosa, v. 13, n. 1, p. 180-204, 2020.

³³⁸ Nesse sentido, a legislação brasileira de proteção de dados prevê, em seu capítulo III, uma série de direitos aos titulares de dados pessoais, entre eles o de acesso aos dados e eliminação dos dados, conforme art. 17 e seguintes da LGPD.

³³⁹ DONEDA, 2019, *op. cit.*, p. 184.

³⁴⁰ Ver tópico 3.2.

assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais”.

Além disso, o *caput* do art. 22 da Constituição Federal também foi reformado, passando a vigorar acrescido do inciso XXVI, estabelecendo competência privativa da União legislar sobre proteção e tratamento de dados pessoais.

A mudanças no texto constitucional tiveram como objetivo, além de organizar a disciplina e promover a proteção de dados pessoais, o de consolidar a autonomia deste direito em relação a previsão geral de proteção à vida privada, prevista no art. 5º, X, da Constituição Federal. Se entendeu que, ainda que uma interpretação normativo-estruturante dos incisos X e XII do art. 5º da Constituição Federal (tutela da vida privada) permitissem a conclusão de que a proteção da vida privada já abrangeria a tutela jurídica da proteção de dados pessoais, a ausência da previsão textual expressa ainda poderia gerar conflitos acerca do âmbito de proteção da norma.³⁴¹

Por se tratar de um conceito jurídico indeterminado e possuidor de subjetividade, a definição de privacidade, conforme visto no tópico 2.4, depende do tempo, local, contexto social e político em que está inserido na sociedade, de forma que se torna difícil determinar exatamente o que está englobado neste direito. Marcel Leonardi sustenta que a privacidade não é uma mera prerrogativa individual de caráter subjetivo, mas engloba, preponderantemente, o que a sociedade considera apropriado proteger.³⁴²

Ainda que a proteção de dados pessoais esteja englobada no conceito da privacidade, sua definição autônoma como um direito fundamental permite que as peculiaridades do termo sejam atendidas, especialmente diante das novas fronteiras da tecnologia. Contudo, a inclusão desse direito fundamental de forma expressa na CRFB tem a capacidade de transformá-lo em uma cláusula pétrea, impedindo qualquer mudança no sentido de limitá-lo.

O significado da alteração legal para futuras decisões judiciais envolvendo a proteção de dados pessoais também deve ser observado, vez que os magistrados agora contam com uma norma expressa na Constituição para a

³⁴¹ MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. 1. ed. São Paulo: Saraiva, 2013. p. 174.

³⁴² LEONARDI, Marcel. **Tutela da privacidade na internet**. São Paulo: Saraiva, 2011. p. 75.

efetiva proteção desses direitos, e não apenas a análise de legislações infraconstitucionais como o CDC, Lei de Acesso à Informação, Lei do Cadastro Positivo, Marco Civil da Internet e LGPD.

Por fim, o reconhecimento do direito fundamental à proteção de dados também pode trazer consequências nos controles difuso e concentrado de constitucionalidade, a caracterização mais clara desse direito em sua dimensão coletiva³⁴³, além de evitar divergências na sua interpretação uma vez estabelecida a competência privativa da União para legislar sobre o tema, impedindo que estados e municípios definam questões específicas relacionadas ao tema.

3.2. REGIME DE PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

O regime de proteção de dados pessoais no Brasil passou por profundas mudanças nos últimos anos, especialmente após a publicação da Lei 13.709/2018, que estabeleceu um marco regulatório na temática da proteção de dados brasileira e alinhou o Brasil junto aos países que contam com uma lei geral que estabelece regras, princípios, bases legais e cria uma autoridade administrativa para fiscalizar e aplicar penalidades em caso de violações envolvendo o tratamento de dados pessoais.

Entretanto, mesmo antes da edição da referida lei, houve um intenso desenvolvimento dessa temática na prática jurídica brasileira, especialmente nas últimas três décadas, seja no âmbito da jurisprudência ou por iniciativas legais e infralegais. Esse processo evolutivo, embora por muito tempo associado especificamente ao direito à privacidade previsto na CRFB e toda sua carga individualista e subjetiva³⁴⁴, assimilou conceitos da proteção de dados pessoais.

Na jurisprudência, muito antes da LGPD, foi possível identificar uma evolução da interpretação do direito à privacidade no sentido de um direito ao controle das próprias informações pessoais devido as modificações sociais e tecnológicas, inclusive no sentido da existência de um direito fundamental à

³⁴³ É o exemplo do art. 22 da LGPD, que estabelece que a “defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.”

³⁴⁴ DONEDA, Danilo. Panorama histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 11.

proteção de dados a partir da interpretação conjunta do art. 5º, X e LXXII, da CRFB.³⁴⁵

No plano constitucional, outro exemplo desse processo que culmina na utilização de conceitos de proteção de dados pessoais no Brasil é a presença da ação de *habeas data* na Constituição de 1988. O instituto, previsto em seu art. 5º, LXXII, prevê uma espécie de direito de acesso e retificação dos dados, conforme redação:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

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;³⁴⁶

Segundo Danilo Doneda, embora a existência do instituto do *habeas data* ser um importante marco constitucional, sua utilização para essas finalidades acabou por não ganhar relevância no plano prático, não obtendo êxito em acompanhar a dinâmica e as mudanças proporcionadas pelo aumento no tratamento de dados pessoais no contexto da Sociedade Informacional.³⁴⁷

A primeira lei que trata de fato de forma moderna sobre alguns aspectos de proteção de dados pessoais no Brasil é o Código de Defesa do Consumidor (Lei n. 8.078/90). Essa legislação, além de estabelecer normas de proteção ao consumidor, estabelece princípios interpretativos de proteção de dados, além criar um sistema de tutela concreta com base no Sistema Nacional de Defesa do Consumidor, com competência para tratar de questões relativas a tratamento de dados pessoais nas relações de consumo.³⁴⁸

Especificamente, o art. 43 do referido Código, regula os bancos de dados e cadastros de consumidores nos seguintes termos:

³⁴⁵ MENDES, *op cit.*, p. 140.

³⁴⁶ BRASIL. **Constituição da República Federativa do Brasil, 1988**. Brasília-DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 mar. 2022.

³⁴⁷ DONEDA, 2021, *op. cit.*, p. 13.

³⁴⁸ DONEDA, 2021, *op. cit.*, p. 14.

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.

§ 1º 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.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º 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.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º 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.

§ 6º 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. (Incluído pela Lei nº 13.146, de 2015) (Vigência)

Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor.

§ 1º É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado.

§ 2º Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.³⁴⁹

Segundo a leitura do dispositivo, é possível concluir pela existência de direitos de acesso e retificação, pelo consumidor, à bancos de dados que contenham informações pessoais a seu respeito. Não obstante, observa-se pela obrigatoriedade de que os cadastros sejam claros, objetivos e verdadeiros, revelando princípios de qualidade e exatidão dos dados. A transparência também é exigida conforme há a necessidade de comunicação da abertura de cadastro ou registro de dados pessoais de consumo, bem como é exigido um limite temporal para o armazenamento dos dados.

A previsão desses direitos e, ainda que não explícitos, princípios de proteção de dados no Código de Defesa do Consumidor (CDC), foi e é

³⁴⁹ BRASIL. **Lei 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/l8078compilado.htm; Acesso em 13 nov. 2022.

largamente utilizado no Brasil para consolidar “o entendimento acerca da existência do direito do consumidor sobre seus dados pessoais”.³⁵⁰

Outra legislação que compõe o regime de proteção de dados pessoais no Brasil é a Lei do Cadastro Positivo (Lei n. 12.414/2011), que, assim como o CDC, estabelece princípios como o da qualidade dos dados pessoais (art. 3º), finalidade (art. 2º, I, 5º, VII e 7º), e direitos de acesso, retificação e cancelamento dos dados (art. 5º, II e III).³⁵¹

Não obstante, é possível observar a presença de um conceito de dados pessoais sensíveis, conforme redação do art. 3º, §3º, II:

Ficam proibidas as anotações de: [...]

II -informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.³⁵²

A principal característica da Lei do Cadastro Positivo (LCP) foi o fato dessa lei ser a primeira normativa brasileira a ser criada nos moldes da sistemática de proteção de dados pessoais já consolidada em outros países, contendo, conforme analisado acima, inúmeros conceitos e princípios de proteção de dados.³⁵³

Em relação aos dados geridos pelo poder público, cumpre examinar a Lei de Acesso à Informação (Lei n. 12.527/2011), que entrou em vigor em 2012 com o objetivo de “propiciar mais transparência à Administração Pública, ampliando o controle dos cidadãos sobre o Estado e concretizando o direito fundamental à informação garantido constitucionalmente”.³⁵⁴

A referida legislação estabelece, em seu art. 31, um regramento específico de proteção de dados pelo poder público:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

³⁵⁰ DONEDA, 2021, *op. cit.*, p. 15.

³⁵¹ MENDES, *op. cit.*, p. 145.

³⁵² BRASIL. **Lei 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplimento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília-DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/12414.htm. Acesso em 13 nov. 2022.

³⁵³ DONEDA, 2021, *op. cit.*, p. 15.

³⁵⁴ MENDES, *op. cit.*, p. 148

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.³⁵⁵

O art. 31 da Lei de Acesso à Informação (LAI) confere, portanto, um direito geral de acesso à informação de forma a regular o princípio da transparência previsto constitucionalmente, além de permitir aos indivíduos a possibilidade de acessar suas informações mantidas pelo poder público em prazos e condições previstas na lei.

Em relação ao direito de acesso de terceiros a informações pessoais, há o estabelecimento de um limite, de modo que não seja possível o acesso destes a dados pessoais armazenados pela Administração Pública sem que haja previsão legal ou o consentimento do titular dos dados, com exceção das hipóteses previstas no art. 31, §3º, ou após o prazo de 100 anos, no caso de dados pessoais relacionados a agentes públicos.³⁵⁶

Outro importante símbolo na evolução da matéria da proteção de dados pessoais no Brasil é o Marco Civil da Internet (Lei n. 12.965/2014), que

³⁵⁵ BRASIL. **Lei 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília-DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 nov. 2022.

³⁵⁶ MENDES, *op cit.*, p. 155.

estabelece um regime de direitos para o usuário da Internet. Apesar de não ser sua intenção regular a temática de proteção de dados de forma abrangente, a referida lei implementou direitos e procedimentos relacionados ao tratamento de dados pessoais, estabelecendo, por exemplo, a proteção destes como princípio da lei (art. 3º, III). Não obstante, há a referência explícita a alguns direitos relativos à proteção de dados, como a necessidade de exatidão dos dados (art. 7º, VI) e direito de eliminação dos dados (Art. 7º, X).

Nota-se, também, que o Marco Civil da Internet (MCI) estabeleceu uma série de procedimentos relacionados ao tratamento de dados pessoais, criando a necessidade de consentimento do titular para o tratamento de dados (art. 7º, IX). Existe, todavia, uma importante diferença entre a referida lei e a posterior entrada em vigor da LGPD. Enquanto o MCI traz uma grande carga valorativa ao consentimento, estabelecendo esta como principal hipótese de tratamento de dados na lei, a LGPD elenca uma série de bases legais em seu art. 7º, sem dar qualquer valoração ou ordem de importância em relação às bases legais de tratamento.

Todas as legislações citadas são importantes marcos e continuam compondo o regime de proteção de dados pessoais no Brasil, mas, de fato, é com a LGPD que diversos elementos novos são introduzidos no ordenamento jurídico brasileiro, sistematizando a problemática relacionada ao tratamento de dados pessoais e todos os riscos gerados por essa atividade no contexto da Sociedade Informacional.

A LGPD buscou definir, de forma detalhada, quem são os agentes de tratamento, separando, por exemplo, os conceitos e responsabilidades do controlador e operador de dados³⁵⁷, e criando uma extensiva enumeração de fundamentos e princípios da lei. Desses, para os fins aqui propostos, pode-se destacar: (i) boa-fé nas relações entre os agentes de tratamento; (ii) finalidade, necessidade e transparência na realização de tratamentos de dados pessoais e; (iii) segurança, prevenção, responsabilização e prestação de contas.

³⁵⁷ Segundo o art. 5º, VI e VII da LGPD, controlador é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, enquanto o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Conforme visto sobre o MCI, a LGPD abandona a carga valorativa dada ao consentimento como principal fundamento de autorização para o tratamento de dados pessoais no ordenamento jurídico brasileiro, criando diversas hipóteses de tratamento de dados em seu art. 7º:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

- I - Mediante o fornecimento de consentimento pelo titular;
- II - Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV - Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V - Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI - Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
- VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
- IX - Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
- X - Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.³⁵⁸

A legislação também determina um regramento específico para o tratamento de dados sensíveis e de crianças e adolescentes, elencando hipóteses de tratamento particulares para essas categorias especiais de dados pessoais, respectivamente, em seus arts. 11 e 14.³⁵⁹

³⁵⁸ BRASIL, República Federativa do. Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, 2018.

³⁵⁹ Art. 11, LGPD: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
 - a) cumprimento de obrigação legal ou regulatória pelo controlador;
 - b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

Por fim, e não pretendendo esgotar a análise das inúmeras inovações trazidas pela LGPD para o regime de proteção de dados pessoais no Brasil, a criação da Autoridade Nacional de Proteção de Dados, com autonomia técnica e decisória, foi fundamental para a fiscalização dos princípios, regras e requisitos para a proteção das informações desta natureza.

Segundo Danilo Doneda, é a LGPD que provê respostas regulatórias efetivamente isonômicas para todas as atividades e setores aos quais ela é aplicável, seja no setor público ou privado, proporcionando um instrumental jurídico próprio para que a lei seja efetiva nos mais diversos ambientes regulatórios.³⁶⁰

Com ela, novos princípios e institutos de proteção de dados passam a vigorar, criam-se direitos específicos aos titulares de dados, além de regras de prestação de contas (*accountability*) para controladores e operadores de dados pessoais.

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

³⁶⁰ DONEDA, 2021, *op. cit.*, p. 19.

O risco das atividades passa a ser considerado um elemento fundamental para a definição da carga de participação do titular no tratamento de dados, além da necessidade de oferecimento de garantias pelas organizações que realizam esses tratamentos.

3.3. A RELAÇÃO DOS RISCOS COM A LGPD

A LGPD impõe uma série de requisitos às organizações que realizam atividades de tratamento de dados de risco, como, por exemplo, a condução de um Relatório de Impacto à Proteção de Dados (RIPD) e a notificação à ANPD caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48, LGPD).

Não obstante, o RGPD, em seu artigo 33, também requer dos controladores de dados um RIPD. O regulamento europeu, no entanto, é mais específico ao definir que somente atividades classificadas como de “alto-risco” ensejarão a condução do relatório:

First, Article 33 requires controllers to conduct a data protection impact assessment for high-risk processing activities. These are processing activities that rely on new technologies and are “likely to result in a high risk for the rights and freedoms of individuals.” Three examples of high-risk activities are provided, including (1) “systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual,” (2) “processing on a large scale of special categories of data,” and (3) “a systematic monitoring of a publicly accessible area on a large scale.” The supervisory authority in each member state may promulgate a list of other processing activities that require data protection impact assessments as well as activities that are specifically exempt from the requirement.³⁶¹

³⁶¹ Tradução livre: Em primeiro lugar, o artigo 33.º exige que os responsáveis pelo tratamento efetuem uma avaliação do impacto da proteção de dados para atividades de processamento de alto risco. Essas são atividades de processamento que dependem de novas tecnologias e “provavelmente resultarão em alto risco para os direitos e liberdades dos indivíduos”. São fornecidos três exemplos de atividades de alto risco, incluindo (1) “avaliação sistemática e ampla de aspectos pessoais relacionados a pessoas físicas que se baseia no processamento automatizado, incluindo a criação de perfis, e na qual se baseiam decisões que produzem efeitos jurídicos sobre o indivíduo ou afetam significativamente o indivíduo”, (2) “processamento em grande escala de categorias especiais de dados” e (3) “monitoramento sistemático de uma área publicamente acessível em grande escala”. A autoridade supervisora em cada estado membro pode promulgar uma lista de outras atividades de processamento que requerem avaliações de impacto de proteção de dados, bem como atividades que são especificamente isentas do requisito (MALDOFF, Gabriel. **The Risk-Based Approach in the GDPR: Interpretation and Implications.** IAPP, [S.l.], 2019. Disponível em:

Nesse sentido, controladores e operadores de dados pessoais devem implementar avaliações de impacto com a descrição dos processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, apresentando as medidas técnicas, organizacionais e mecanismos que garantam uma adequada mitigação dos riscos relacionados ao tratamento de tais dados. Sobrevém que a LGPD não descreveu, de forma objetiva, quais são as atividades que ensejam essa avaliação formal de risco, descrita no art. 5º, XVII, da LGPD.

Essa definição depende de uma interpretação sistemática da legislação, identificando as categorias de dados pessoais e tipos de operações de tratamento que podem, em maior ou menor medida, gerar um elevado grau de risco aos titulares devido às circunstâncias do seu tratamento, como, por exemplo, o *profiling*³⁶², tratamento de dados em larga escala, uso de dados públicos e dados bancários ou financeiros.

As tecnologias trabalhadas no capítulo 2 (dois) e a hiperconectividade consequente do seu uso, como o *Big Data*, a Internet das Coisas e técnicas de IA, a exemplo do *Machine Learning*, são particularmente relevantes sob a perspectiva da necessidade de uma análise de impacto dos riscos inerentes ao seu uso.

A Internet das Coisas, por exemplo, ao permitir que dispositivos físicos dos mais diversos tipos, conectados à Internet, monitorem de forma permanente os ambientes e indivíduos a sua volta, é suscetível a eventuais falhas (sejam elas provocadas por agentes externos ou não), tornando-se, assim, um relevante vetor de risco para as organizações públicas ou privadas que fazem uso desse tipo de tecnologia, bem como para os indivíduos afetados. Nesse sentido, há um

https://iapp.org/media/pdf/resource_center/The_Risk-Based_Approach_in_the_GDPR_Interpretation_and_Implications.pdf. Acesso em: 27 nov. 2022.)

³⁶² Refere-se “aos métodos e técnicas computacionais aplicados aos dados pessoais ou não dos usuários”. São técnicas que tem como objetivo “o que é relevante dentro de um contexto, por exemplo, quem pode estar interessado em determinado produto. Cf.: BOFF; FORTES; FREITAS, *op. cit.*, p. 168)

risco considerável na utilização de tais tecnologias, que, se não levados em conta, podem gerar consequências nefastas em um amplo aspecto de direitos.³⁶³

O *Big Data* e o processamento de dados por meio de técnicas de IA, também analisadas no tópico 2.2, podem levar à exclusão de grupos inteiros do acesso a direitos e serviços com base em modelos preditivos potencialmente enviesados. Os impactos ao livre desenvolvimento da personalidade decorrentes dessas inteligências preditivas, bem como dos eventuais riscos à democracia por conta da capacidade de vigilância facilitadas por essas tecnologias, levantam importantes perguntas sobre a segurança, privacidade e responsabilidade no uso dessas ferramentas, motivo pelo qual se mostra necessário que elas sejam sistematicamente avaliadas para que haja uma efetiva compatibilidade com a LGPD e demais fundamentos constitucionais da privacidade e outros direitos da personalidade.³⁶⁴

O tratamento de dados pessoais sensíveis deve ser realizado com cautela e mediante o cumprimento de diferentes requisitos previstos na LGPD, devido ao potencial discriminatório dessa categoria de informação. Tais dados apresentam uma ameaça em potencial do ponto de vista dos direitos e liberdades fundamentais. Ou seja, o seu uso, independente do contexto, propicia riscos significativos ao seu titular.

Embora a LGPD tenha elencado um rol taxativo de dados pessoais considerados sensíveis³⁶⁵, para se determinar se um dado é sensível ou não, é essencial verificar o contexto da sua utilização, bem como quais as relações entre dados que podem ser realizadas e a potencialidade do tratamento ser utilizado para fins de estigmatização ou discriminação.³⁶⁶

Nesse sentido, dados comuns podem ser considerados sensíveis quando eles contribuem para a elaboração de um perfil que possa gerar um prejuízo à

³⁶³ BELLI, Luca. Como implementar a LGPD por meio da avaliação de impacto sobre privacidade e ética de dados. In: DONEDA, Danilo. Panorama histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 397.

³⁶⁴ *ibid.*, p. 399.

³⁶⁵ São dados pessoais sensíveis, segundo art. 5º, II, LGPD: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

³⁶⁶ TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021. p. 138.

esfera individual da pessoa, especialmente caso o perfil traçado tenha conotações negativas e possa gerar discriminação.³⁶⁷

Já os dados de crianças e adolescentes devem ser utilizados no seu melhor interesse, bem como mediante o consentimento parental no caso de crianças menores de doze anos.³⁶⁸ Nesse sentido, o tratamento de tais dados pode se dar exclusivamente por meio de práticas que “promovam e protejam seus direitos previstos no sistema jurídico nacional e internacional com absoluta prioridade, abstendo-se de práticas violadoras e exploratórias da vulnerabilidade infantojuvenil, inclusive as comerciais”. Assim, é importante observar que o considerando 38 do RGPD define que as crianças merecem especial proteção quanto aos seus dados pessoais por estarem menos cientes dos riscos, consequências e garantias em relação aos seus direitos, especialmente em casos de uso de tais dados com finalidades de comercialização, acesso a serviços ou criação de perfis.³⁶⁹

Esses exemplos de categoria de dados pessoais geram, por sua natureza intrínseca, maiores riscos quando utilizados por agentes controladores e operadores de dados pessoais. Há, porém, situações em que a própria operação de tratamento, independente do seu conteúdo, gera um risco ao titular de dados pelas características da operação.

É o exemplo da transferência internacional de dados, que só poderá ser realizada quando: (i) o país de destino dos dados pessoais possuir nível de proteção de dados pessoais adequado ou; (ii) quando o controlador oferecer e comprovar garantias de cumprimento dos princípios e direitos dos titulares

³⁶⁷ RODOTÁ, *op cit.*, p. 84.

³⁶⁸ A necessidade de consentimento se aplica somente a crianças, ficando de fora essa restrição aos adolescentes (maiores de 12 anos). Esse é o entendimento do Relatório da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei 4.060/2012 (que posteriormente resultou na LGPD), em que é claro ao determinar que a exigência mais elevada de consentimento é restrita ao caso de tratamento de dados de crianças. Cf.: MALDONADO, Viviane Nóbrega; OPICE, Renato Opice. **Lei Geral de Proteção de Dados Pessoais** Comentada. 3. ed. Revista dos Tribunais. São Paulo: 2021. p. 221.

³⁶⁹ Segundo o considerando: “As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilização, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.”

previstos na LGPD. Portanto, a organização que transfere dados internacionalmente deve, antes de realizar a transferência, avaliar se o país de destino conta com uma legislação de proteção de dados equivalente à LGPD ou, não sendo o caso, utilizar cláusulas contratuais específicas, padrão ou normas corporativas globais aptas a garantir que as normas de proteção de dados brasileiras serão observadas na organização de destino dos dados.³⁷⁰

Por fim, o uso da base legal do legítimo interesse (art. 7º, IX, LGPD) também demandará uma avaliação de risco criteriosa para determinar se os interesses legítimos do controlador devem prevalecer em relação aos direitos e liberdades fundamentais do titular de dados. O uso dessa base legal de tratamento é justificado quando presentes três requisitos fundamentais: “(i) identificar um interesse legítimo (teste de propósito); (ii) mostrar que o processamento é necessário para alcançá-lo (teste de necessidade) e (iii) equilibrá-lo contra interesses, direitos e liberdades do indivíduo (teste de equilíbrio).³⁷¹ O risco, portanto, está diretamente ligado às eventuais falhas em determinar o propósito e necessidade da operação, sem que haja conflitos com os direitos e liberdades fundamentais do titular de dados.

É a relação entre riscos inerentes às operações de tratamento (sejam com categorias especiais de dados pessoais ou características próprias da operação) e as atividades preventivas realizadas pelas organizações que tratam dados que fundamentam os critérios estabelecidos para a Autoridade Nacional de Proteção de Dados avaliar as penalidades em caso de não conformidades, bem como para a atribuição da responsabilidade civil em processos judiciais que aferem a responsabilidade de controladores ou operadores de dados pessoais que tenham violado a legislação de proteção de dados (art. 42, *caput* e §3º, da LGPD).

A LGPD, em vários momentos, prescreve a forma como o controlador ou operador de dados pessoais deve agir. Aqueles agentes de tratamento que agem de forma preventiva e diminuem os riscos da sua operação reduzem,

³⁷⁰ LEONARDI, *op. cit.*, p. 290.

³⁷¹ MAIA, Fernanda Simplicio. Introdução ao Legítimo Interesse. In: DE LUCCA, Newton et al. **Direito & Internet IV**: Sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.p. 307.

consequentemente, sua carga de participação danosa em um eventual incidente envolvendo dados pessoais.

Dessa forma, os controladores e operadores de dados pessoais devem adotar regras de boas práticas levando em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e benefícios decorrentes de tratamento de dados do titular (art. 50, §1º, LGPD).

Pode se dizer, com base na relação do risco com a LGPD, que existe a adoção do modelo regulatório chamado de "risco de conformidade", de modo que, quanto menor a conformidade, maiores as consequências para o agente de tratamento envolvido. Há uma conexão direta entre a conformidade da legislação, a gestão de riscos e a afetação de direitos e liberdades dos titulares de dados.³⁷²

A própria LGPD estabelece, por exemplo, que serão consideradas a adoção de políticas de boas práticas e governança ou medidas corretivas para estabelecer os critérios para aplicação de sanções administrativas em caso de infrações cometidas às normas previstas na lei (art. 52, §1º, LGPD). A ANPD, portanto, ao decidir sobre a aplicação de uma penalidade, deverá considerar o grau de responsabilidade do controlador ou operador de dados, tendo em conta as medidas técnicas e organizacionais implementadas na organização.

Todavia a ANPD deverá considerar a natureza, gravidade e duração da infração tendo em vista a natureza, âmbito ou finalidade do tratamento. Fatores como negligência e dolo também devem ser considerados. Ao demonstrar a adesão a códigos de conduta ou certificações, os agentes de tratamento poderão ter suas penalidades reduzidas, ou mesmo eliminadas. A gestão de risco torna-se, ao lado da própria observância das normas extraídas da lei, uma importante forma de demonstração de conformidade em matéria de proteção de dados pessoais.

Assim, torna-se fundamental, seja para as organizações públicas ou privadas, que sejam desenvolvidos programas de governança em proteção de

³⁷² GELLERT, Raphael. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, [S.l.], v. 33, n. 1, p. 12-23, 2017. Disponível em: <https://doi.org/10.1016/j.clsr.2016.11.007>. p. 6. Acesso em: 27 nov. 2022.

dados e *compliance*, além de ferramentas de mitigação e análise de risco, para que haja uma efetiva tutela da proteção de dados pessoais.

3.4. MITIGAÇÃO DE RISCOS NA SOCIEDADE INFORMACIONAL: FERRAMENTAS DE GESTÃO DE RISCO E *COMPLIANCE*

No tópico sobre a obra do sociólogo alemão Ulrich Beck³⁷³, foi dito que o risco pode ser definido como um perigo possível no futuro. Entretanto, em um contexto de busca por conformidade e governança em proteção de dados, o risco, em seu sentido mais técnico, pode ser descrito como um elemento de auxílio na tomada de decisões com base na avaliação de eventos futuros:

Sem chance de ocorrência futura, um evento hipotético não se configura como risco. Sem impacto negativo significativo, um evento hipotético não se configura como risco. É também importante destacar que, mesmo que um evento futuro negativo tenha 50% de chance de ocorrer e impacto negativo valorado, haverá sempre uma incerteza associada a tal estimativa. Isto é, podemos ter baixa, média ou alta confiança de que o evento tem 50% de chance de ocorrer, bem como podemos ter baixa, média ou alta confiança de que o impacto negativo real será do valor que estimamos.³⁷⁴

Num contexto de governança em proteção de dados, a etapa de identificação de riscos é de suma importância. Desenhar uma matriz de riscos e criar um cronograma de adequação são medidas comuns e eficazes em organizações que buscam mitigar os riscos relacionados ao tratamento de dados pessoais. Essa matriz deverá levar em conta as categorias de dados pessoais (como, por exemplo, dados pessoais sensíveis ou de crianças e adolescentes), as finalidades do tratamento, e os potenciais riscos a liberdades e direitos fundamentais do titular, entre outros fatores:

A matriz também pode ser útil à medida que, quanto maior o nível de risco para os direitos fundamentais do indivíduo que determinada prática representar, maiores serão as medidas necessárias para proteção contra esses riscos. A LGPD não chega a realizar uma lista de formas de tratamento que podem ser consideradas mais danosas, mas indica “a probabilidade e a gravidade dos riscos” como critério a ser considerado no desenvolvimento de medidas de governança (art.

³⁷³ Tópico 1.4.

³⁷⁴ FERNANDAS, Jorge Henrique Cabral. Introdução à gestão de riscos de segurança da informação. >> **Gestão da Segurança da Informação e Comunicações** >> 2009-2011. GSIC302. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf. Acesso em: 02 fev. 2023.

50, §1º), e tal questão é fundamental no desenvolvimento de quaisquer medidas de boas práticas.³⁷⁵

Nesse caso, a LGPD define que controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, procedimentos, normas de segurança, padrões técnicos, ações educativas, mecanismos internos de supervisão e mitigação de riscos, entre outros.³⁷⁶

Tal previsão não detalha, no entanto, de que forma tais regras de boas práticas e governança deverão ser desenvolvidas, embora a lei estabeleça os requisitos mínimos do programa de governança em privacidade:

- 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;³⁷⁷

Existem diversas normas e *frameworks* que podem ser utilizados como ferramentas de planejamento voltado à gestão de programas de conformidade em proteção de dados, como o recomendado pela LGPD. A família ISO 27000, por exemplo, compreende uma série de regras voltadas à segurança da informação e privacidade. Elas são normas “técnicas que fornecem orientação e

³⁷⁵ CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021. p. 368.

³⁷⁶ Art. 50. BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

³⁷⁷ Art. 51. . BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

direção de como uma organização, independentemente de seu porte e setor, deve gerenciar a segurança das informações”, bem como os seus riscos.³⁷⁸

Embora não diretamente voltado para a proteção de dados pessoais, os *frameworks* de governança em tecnologias da informação (TI) também são uma importante forma de prevenir riscos de modo sistematizado nas organizações que realizam tratamento de dados pessoais através do uso das TICs, especialmente por essas manifestarem uma certa “tendência natural” para entrar em conflito com o Direito em relação ao controle da circulação dos dados pessoais (autodeterminação informativa)³⁷⁹. O COBIT (*Control Objectives for Information and related Technology*), por exemplo, é um *framework* de gerenciamento e gestão de riscos que fornece uma estrutura abrangente para a governança e gestão de TI criado pela *Information Systems Audit and Control Association* (ISACA). Trata-se de uma ferramenta de gerenciamento de todo o ambiente computacional, auxiliando a manutenção do equilíbrio entre os seus objetivos e os riscos inerentes à operação da organização.³⁸⁰

Por sua vez, outro importante *framework* de conformidade em TI é o ITIL (*Information Technology Infrastructure Library*), um conjunto de boas práticas e processos para o gerenciamento de serviços de TI. Seu objetivo principal é melhorar a eficiência e os resultados da organização:

ITIL is a set of practices for IT Service Management (ITSM) that identifies and develops actions aiming to improve each provided IT service’s overall quality, efficiency, and effectiveness, reflecting trends in software development and IT operations. It includes recommendations on how to apply philosophies such as Agile, DevOps, and Lean in the service management domain [Axelos and Office 2019]. DevOps seeks to remove technical, process, and cultural barriers between development and operation areas. So, it eliminates blocks, improves collaboration, empowers people, accelerates productivity, and automates. It is more related to People & Processes, but for sure, it also includes tools.³⁸¹

³⁷⁸ FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. **A segurança da informação como ferramenta técnico da proteção de dados pessoais**. Direito e Inovação v. 3. Curitiba: OAB/PR, 2020. p. 245.

³⁷⁹ RODOTÁ, *op. cit.*, p. 113.

³⁸⁰ PEIXE, Adriana Maria Miguel; BALSAN, Jorge; PINTO, José Simão de Paula. Governança Corporativa e Governança de Tecnologia da Informação como vantagem competitiva nas organizações. **Research, Society and Development**. v. 10, n. 5. Disponível em: <https://rsdjournal.org/index.php/rsd/article/view/14636/13169>. Acesso em: 02 fev. 2023.

³⁸¹ Tradução livre: O ITIL é um conjunto de práticas para o Gerenciamento de Serviços de TI (ITSM) que identifica e desenvolve ações com o objetivo de melhorar a qualidade, eficiência e eficácia geral de cada serviço de TI prestado, refletindo tendências no desenvolvimento de software e operações de TI. Inclui recomendações sobre como aplicar filosofias como Agile,

Ambos os *frameworks* possuem propósitos semelhantes, incluindo a melhoria da qualidade dos serviços de TI e a maximização do seu valor para a organização. No entanto, há algumas diferenças fundamentais entre eles. Enquanto o COBIT se concentra em governança de TI, abordando questões de segurança da informação, avaliações de risco e *compliance*, o ITIL se concentra em gerenciamento de processos e serviços de TI. Em resumo, ambos os *frameworks* são complementares e ajudam as organizações a maximizar o valor de sua infraestrutura de informação e a mitigar os riscos derivados da sua operação.³⁸²

A LGPD confere especial atenção, no caso do estabelecimento de regras de boas práticas, ao processo de análise de probabilidade e gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.³⁸³

Uma norma bastante utilizada para auxiliar na identificação dos riscos é a ISO 31000:2018, que estabelece princípios e diretrizes para a gestão de riscos, definidos como as “influências e fatores internos e externos que tornam incerto se e quando elas atingirão seus objetivos. O efeito que essa incerteza tem sobre os objetivos da organização é chamado de risco”.³⁸⁴

O conceito de risco é, portanto, muito amplo, e normalmente se relaciona não só com as suas consequências. Isto é, o impacto que ele causa em determinado contexto. Mais do que isso, o risco engloba fatores como a sua fonte ou origem, as circunstâncias em que ele se desenvolve, bem como a probabilidade de sua ocorrência.

Nesse sentido, o risco, como visto, nada mais é do que uma noção abstrata, necessitando de metodologias, modelos e processos que permitam a

DevOps e Lean no domínio de gerenciamento de serviços [Axelos e Office 2019]. O DevOps busca remover barreiras técnicas, de processo e culturais entre as áreas de desenvolvimento e operação. Assim, elimina bloqueios, melhora a colaboração, capacita as pessoas, acelera a produtividade e automatiza. Está mais relacionado a Pessoas & Processos, mas com certeza também inclui ferramentas. Cf.: CARTURAN, Sara B. O. G.; MATSUI, Beatriz M. A.; GOYA, Denise H.. GPD Framework: An Implementation and *Compliance* Guide for Technology Areas. [Anais...] XLIX Seminário Integrado de Software e Hardware, p. 176-187, 2022. Disponível em: <https://sol.sbc.org.br/index.php/semish/article/view/20807/20633>. Acesso em: 02 fev. 2023.

³⁸² *ibid.*

³⁸³ Art. 50, §1º. BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

³⁸⁴ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 31.000/2018: **Gestão de riscos — Diretrizes**. Rio de Janeiro, 2018. p. 5.

sua tradução em ações cujo objetivo principal é a sua redução, uma vez que comunidade científica geralmente considera impossível reduzir os riscos a um nível zero.³⁸⁵

Assim, a ISO 31000:2018 define uma série de passos para a configuração dos riscos. Segundo a norma, o risco é expresso em quatro termos: i) eventos; ii) consequências; iii) probabilidades e; iv) fontes de risco.³⁸⁶ É a composição dos três primeiros termos (eventos, consequências e probabilidades) que resultam em fontes de risco identificadas. Esse processo é denominado, em sentido amplo, como análise de risco.

A fonte de risco pode ser definida como o elemento que, de forma individual ou combinada, tem o potencial de dar origem ao risco. O evento, por sua vez, é uma “ocorrência ou mudança de um determinado conjunto de circunstâncias”³⁸⁷, podendo ser ele próprio uma fonte de risco, assim como algo que é esperado pela organização. As consequências são também entendidas como “o resultado de um evento”³⁸⁸. Por exemplo, as consequências de um acesso não autorizado a um sistema. Trata-se de uma consequência negativa, embora isso não seja uma regra.³⁸⁹ Por fim, e não tendo a intenção de esgotar o assunto, a probabilidade é classicamente definida como “a chance de algo acontecer”³⁹⁰ e leva em conta fatores de risco, ou seja, como e se ele se materializará, bem como sua gravidade. A ISO a define como “elementos que, isoladamente ou em combinação, têm potencial intrínseco para gerar risco”.³⁹¹

Após a configuração dos riscos, passa-se à análise de risco propriamente dita, que é composta por duas etapas: i) avaliação de risco e; ii) gerenciamento de risco. A primeira mede o nível de risco em termos de probabilidade de sua

³⁸⁵ The decision at risk management level is usually accompanied by measures aiming at reducing the level of risk: sometimes the risk level is too high, but it can be reduced to an acceptable level. These measures can be referred to as risk reduction, risk control, risk response, or more generally, risk mitigation measures. It is commonly accepted that it is impossible to reduce risks to a zero level. So the whole point of the risk management step is to determine whether the level of risk is sufficiently low so that it can be taken (GELLERT, Raphael. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, [S.l.], v. 33, n. 1, p. 12-23, 2017. Disponível em: <https://doi.org/10.1016/j.clsr.2016.11.007>. p. 3. Acesso em: 27 nov. 2022).

³⁸⁶ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 1.

³⁸⁷ *ibid.*, p. 2.

³⁸⁸ *ibid.*, p. 2.

³⁸⁹ Segundo a ISO 31000:2018, as consequências de um evento podem ser certas ou incertas, e podem gerar efeitos positivos ou negativos, diretos ou indireto.

³⁹⁰ *ibid.*, p. 2.

³⁹¹ *ibid.*, p. 4.

ocorrência e a gravidade em caso de sua realização. Já o gerenciamento de risco consiste na tomada de decisão em assumir riscos ou não. Essa tomada de decisão normalmente é acompanhada por medidas que visam reduzir os níveis de risco (medidas de mitigação de risco), para então determinar se o nível de risco é suficientemente baixo para que ele possa ser assimilado pela organização.³⁹²

Na primeira etapa de uma avaliação de riscos, é necessária a descrição de um número abrangente de situações de riscos da organização que servirá como base para todas as demais etapas do processo. Essa etapa pode ser definida como o “processo de localização, reconhecimento e descrição de riscos” e é chamada de “etapa de identificação de riscos”.³⁹³

Trata-se de uma atividade crucial, sendo essencial que a organização inclua todos os potenciais riscos, ainda que sua fonte não esteja sob o seu controle. Em outras palavras, essa etapa tem como objetivo “comparar as características do evento em causa com as estabelecidas nos critérios de risco, e que irão determinar se o evento é suficientemente arriscado para ser considerado um risco”.³⁹⁴

Esse processo de identificação de riscos tem destaque nos guias operacionais para adequação à LGPD disponibilizados pela Secretaria de Governo Digital³⁹⁵. No *template* fornecido pelo grupo de trabalho sobre o RIPD, há expressa menção à etapa de identificação de riscos, no sentido de que, antes de descrever quais medidas de mitigação de risco serão adotadas pela organização, “é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais”.³⁹⁶

A Norma ISO/IEC 29134:2017, que estabelece requisitos de Segurança da Informação e guias para avaliação de risco em privacidade, traz uma lista exemplificativa de riscos ligados à proteção de dados pessoais, conforme a Tabela 01.

³⁹² *ibid.*, p. 5.

³⁹³ *ibid.*, p. 5.

³⁹⁴ GELLERT, *op. cit.*

³⁹⁵ BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Segurança e Proteção de Dados – Guias e modelos**. 2021. Disponível em: <https://www.gov.br/gestao/pt-br>. Acesso em: 13 nov. 2022.

³⁹⁶ *Template* disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_template_ripd.docx/view.

Tabela 1 - Riscos ligados ao tratamento de dados pessoais³⁹⁷

ID	Risco referente ao tratamento de dados pessoais
1	Acesso não autorizado.
2	Modificação não autorizada.
3	Perda.
4	Roubo.
5	Remoção não autorizada.
6	Coleção excessiva.
7	Informação insuficiente sobre a finalidade do tratamento.
8	Tratamento sem consentimento do titular dos dados pessoais (caso o tratamento não esteja previsto em legislação ou regulação pertinente).
9	Falha em considerar os direitos dos titulares de dados pessoais.
10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.
11	Retenção prolongada de dados pessoais sem necessidade.
12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.

Uma vez identificados os riscos, parte-se para a etapa de análise propriamente dita, cujo objetivo é desenvolver a compreensão dos riscos para a organização. Seu principal propósito é ser uma entrada para a avaliação de riscos e para a tomada de decisões sobre a necessidade de tratá-los, bem como estratégias e métodos mais adequados para a sua mitigação.³⁹⁸

Se um evento for considerado um risco para a organização, ele deve passar por uma avaliação para determinar seu nível em termos de probabilidade e impacto.³⁹⁹ Nesse sentido, a função da análise de risco é apreciar as causas e as fontes de risco, bem como “suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer.”⁴⁰⁰ Essa análise é

³⁹⁷ Adaptado de ISO/IEC 29134:2017.

³⁹⁸ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 17.

³⁹⁹ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 5.

⁴⁰⁰ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 17.

geralmente realizada segundo uma matriz de probabilidade de um evento ocorrer *versus* o impacto caso ele se concretize.

Uma vez realizada a análise dos riscos, estabelecendo a probabilidade e o impacto dos eventos, chega o momento em que a organização deve tomar uma decisão sobre o risco gerado. Assim, a principal finalidade da avaliação de riscos é auxiliar a organização na tomada de decisões com base nos resultados dessa avaliação, estabelecendo uma ordem de prioridade para a implementação de medidas de mitigação de risco ou monitoramento deste.

Nesse aspecto, “a avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado”.⁴⁰¹ É com base nessa avaliação que decisão será tomada, avaliando a necessidade de executar uma medida de mitigação de risco.

A decisão deverá tomar como base todas as etapas anteriormente descritas, bem como um contexto mais amplo do risco, considerando, entre outros fatores, a tolerância da organização e seus *stakeholders* aos riscos, os benefícios retirados da sua assunção e os requisitos legais ou regulatórios aplicáveis ao caso concreto, como, por exemplo, a LGPD e eventuais leis setoriais aplicáveis.

Em determinados contextos, a avaliação de riscos poderá levar a organização à decisão de não tratar o risco de nenhuma outra forma, mantendo apenas os controles existentes e monitorando essa atividade de forma crítica. Dessa avaliação procederá o gerenciamento do risco, ou seja, “será avaliado em termos de seus custos e benefícios. Haverá a decisão de tomá-la ou não, eventualmente com recurso a medidas de mitigação de risco”.⁴⁰²

Entre as medidas de gerenciamento de risco, pode estar a adoção de ações que visem proteger os dados pessoais e garantir os direitos dos titulares na própria concepção de produtos e serviços de organizações. Esse tipo de ação não só é recomendado pela própria legislação de proteção de dados, como também faz parte de um modelo de regulação que visa responder, para além do Direito, aos riscos criados pela Sociedade Informacional.

⁴⁰¹ ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 18.

⁴⁰² ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, *op. cit.*, p. 6.

3.5. O *PRIVACY BY DESIGN* E A REGULAÇÃO POR ARQUITETURA COMO RESPOSTA AOS RISCOS CRIADOS PELA SOCIEDADE INFORMACIONAL

A questão da regulação em ambientes inovadores não é nova. Como visto no capítulo 2 (dois), a Internet, em sua gênese, foi considerada um local sem qualquer autoridade clara. Nesse período, a pequena comunidade de usuários da rede a enxergava como um espaço autônomo, onde o governo não era bem-vindo.⁴⁰³ Marcel Leonardi afirma em sua obra sobre tutela e efetividade na internet que, apesar da percepção inicial da internet como “espaço livre e separado dos territórios físicos, imune à soberania dos Estados organizados”,⁴⁰⁴ prevaleceu a ideia de que a internet não é um lugar,⁴⁰⁵ mas um meio de comunicação que conecta intermediários através de uma representação audiovisual de coisas reais.⁴⁰⁶ A discussão sobre a regulamentação ou não da internet foi superada e deu lugar ao debate sobre como ela deveria ser regulamentada.⁴⁰⁷

A LGPD, em seu artigo 46, §1º, trata sobre a adoção de medidas de segurança técnicas e administrativas para proteger os dados pessoais dos titulares, por parte dos agentes de tratamento.⁴⁰⁸ Isso nada mais é do que regular as medidas técnicas a serem utilizadas pelas organizações para a proteção de dados pessoais contra acessos não autorizados, destruição, perda, alteração,

⁴⁰³ A ideia de uma Internet como local livre de qualquer intervenção estatal foi inicialmente concebida por John Perry Barlow em artigo denominado “A Declaration of the Independence of Cyberspace”. Cf.: BARLOW, John Perry. A Declaration of the Independence of Cyberspace. In: **Electronic Frontier Foundation**, 1996. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 02 dez. 2022.

⁴⁰⁴ LEONARDI, *op. cit.*, p. 126.

⁴⁰⁵ Inicialmente, este local independente foi denominado “Ciberespaço”. Cf.: LEONARDI, *op. cit.*, p. 126.

⁴⁰⁶ *ibid.*, p. 129.

⁴⁰⁷ Topologia: forma ou configuração de uma rede de aparatos tecnológicos, por exemplo, computadores. Ver em: LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. Rio de Janeiro: Livros Técnicos e Científicos S.A., 1999. pp. 150-152.

⁴⁰⁸ Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. [...] § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei.

comunicação, seja de forma acidental ou ilícita, ou qualquer outra forma de tratamento inadequado ou ilícito de dados pessoais.⁴⁰⁹

Essas medidas devem ser efetivadas desde a fase de concepção do produto ou do serviço até a sua execução. Ou seja, desde a fase de desenvolvimento do produto ou serviço em questão.⁴¹⁰ Essa medida de segurança prevista pela LGPD tem o propósito de reduzir consideravelmente os riscos relacionadas à tutela da privacidade e, conseqüentemente, os riscos tecnológicos da LGPD.

Tal previsão é um movimento de leis de proteção de dados, inclusive o RGPD⁴¹¹, que efetiva o *Privacy by Design* (PdD), conceito criado nos anos 2000 pela então Comissária de Privacidade de Ontário/Canadá, Ann Cavoukian, como modelo regulatório que estabelece sete princípios articuladores entre leis de proteção de dados pessoais e códigos de softwares de produtos ou serviços.⁴¹²

⁴⁰⁹ Art. 46. BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

⁴¹⁰ Art. 46 § 2º As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Cf.: BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

⁴¹¹ Tal previsão encontra-se no art. 25 da referida legislação: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

1The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. 2That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. 3In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate *compliance* with the requirements set out in paragraphs 1 and 2 of this Article.

⁴¹² BIONI, Bruno Ricardo. Abrindo a "caixa de ferramentas" da LGPD para dar vida ao conceito ainda elusivo de *privacy by design*. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019. P. 241.

A ideia do PbD parte, portanto, da concepção de que o Direito não é autossuficiente para alterar comportamentos sociais, sendo necessário articular esses processos restritivos junto com a própria tecnologia.⁴¹³

O professor de Harvard Lawrence Lessig, em sua obra de referência sobre a regulação na Internet denominada *Code: and other laws of cyberspace*, foi um dos precursores ao demonstrar que a simples influência da lei não seria suficiente para regular o ambiente da Internet.⁴¹⁴ O autor dá o exemplo da proibição de jogos online, não bastando uma vedação legal para coibir sua prática, mas, também, uma articulação com a tecnologia de sistemas de pagamento e eventual responsabilização das operadoras de cartão de crédito.⁴¹⁵ Nesse sentido, segundo o referido professor, não é só o Direito que influencia comportamentos por meio das consequências jurídicas de um ato. As normas sociais, o mercado e, principalmente, a arquitetura,⁴¹⁶ são importantes para que o comportamento humano seja afetado e condutas indesejadas sejam mitigadas.

O Direito, por ter prevalência na regulação sobre todas as outras frentes, assume um papel central, mas não estanque para a efetividade das leis. A arquitetura é, portanto, uma modalidade alternativa de regulação, na medida em que as características de determinadas coisas fazem com que comportamentos sejam restringidos ou condutas forçadas, sem qualquer dependência de cooperação ou mesmo de capacidade coercitiva do Estado.⁴¹⁷

⁴¹³ BIONI, Bruno Ricardo. Abrindo a “caixa de ferramentas” da LGPD para dar vida ao conceito ainda elusivo de privacy by design. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019. P. 241.

⁴¹⁴ LESSIG, Lawrence. **Code: and other laws of cyberspace**. New York: Basic Books, 2006. p. 3.

⁴¹⁵ BIONI, Bruno Ricardo. Abrindo a “caixa de ferramentas” da LGPD para dar vida ao conceito ainda elusivo de privacy by design. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019. P. 241.

⁴¹⁶ O conceito de arquitetura deve ser entendido como a resolução de problemas do cotidiano com o uso de soluções por meio da arquitetura física das coisas. Se é necessário reduzir a velocidade de veículos em uma via, lombadas são inseridas na via para dificultar ou impedir o tráfego em alta velocidade. Se um ambiente deve ser acessível para cadeirantes, um elevador ou uma rampa de acesso devem ser instalados. Esses são exemplos que demonstram o modo como a arquitetura das coisas são um regulador mais efetivo, na maioria das vezes, do que simples comandos legais. Assim, a ideia de arquitetura deve ser entendida em um sentido amplo, pois ela representa o mundo como ele é, como as coisas se comportam e se apresentam na natureza, bem como o ser humano as projeta e constrói. Nesse sentido, Marcel Leonardi explica que a arquitetura “é uma modalidade de regulação na medida em que as características de determinadas coisas restringem comportamentos ou forçam determinadas condutas. Cf: LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p. 161.

⁴¹⁷ LEONARDI, Marcel. **Tutela e Privacidade na Internet**. São Paulo: Saraiva, 2012. p. 157.

Quando o tratamento de dados pessoais envolve, por exemplo, o desenvolvimento de código-fonte (*software*), entende-se que o legislador tomou a segurança e o sigilo de dados para, verdadeiramente, incentivar o modelo de *Privacy by Design*, com princípios que utilizam a arquitetura própria de proteção de dados ainda na fase de desenvolvimento dos produtos e serviços relativos a dados pessoais, tornando-os mais seguros e acessíveis aos usuários.⁴¹⁸

O *Privacy by Design* nada mais é do que sistemas de informação desenvolvidos de forma a prever, já em seu código-fonte – ou seja, em sua arquitetura - todas as metodologias e técnicas necessárias para a proteção dos dados pessoais e da privacidade do usuário, estabelecendo padrões restritivos de coleta de dados atrelados ao conceito do mínimo necessário, exercício dos direitos dos titulares, bem como a previsão de processos de anonimização de dados pessoais, quando necessário⁴¹⁹. Esse conjunto de regras definidas já no momento de concepção do produto ou serviço busca “a criação de confiança não apenas no método, no procedimento de coleta e de tratamento de dados, mas também na própria arquitetura do sistema”.⁴²⁰

Se no mundo real a arquitetura das coisas funciona como um regulador e limitador do comportamento humano, o código-fonte exerce esse papel no contexto das TICs. Ele está presente nos *softwares* e aplicativos e pode ser inclusivo ou exclusivo, justo ou injusto. O código define como os dados pessoais serão coletados, em que medida serão processados e em que momento serão excluídos. Por fim, a depender da arquitetura de código adotada em um

⁴¹⁸ Ann Cavoukian aponta sete princípios norteadores da concepção de *privacy by design*: 1) adoção de medidas proativas e preventivas, não reativas, a fim de remediar as situações; 2) Privacidade como *default*, ou seja, como padrão; 3) Privacidade inserida no *design* e na arquitetura do sistema de tecnologia da informação e nas práticas de negócio; 4) Funcionalidade completa, de modo que o resultado seja benéfico, não nulo; 5) Segurança de ponta a ponta; 6) Visibilidade e transparência; e 7) Respeito pela Privacidade do usuário. Cf.: CAVOUKIAN, Ann. *Privacy by design: The 7 foundational principles*. **Information and Privacy Commissioner of Ontario**, Canada, v. 5, 2009.

⁴¹⁹ Conforme art. 6º da LGPD, o conceito de mínimo necessário pode ser entendido como a limitação do tratamento ao mínimo necessário para a realização de suas finalidades, conforme os dados estritamente pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

⁴²⁰ LEMOS, Ronaldo; BRANCO, Sérgio. *Privacy by Design: conceito, fundamentos e aplicabilidade na LGPD*. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES, Otavio Luiz; BIONI, Bruno (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2021. p. 450.

determinado sistema, ele poderá ignorar ou promover a proteção de dados e a privacidade dos seus usuários.⁴²¹

O autor Bruno Bioni descreve um exemplo interessante de PbD em seu livro "*Proteção de Dados Pessoais: a função e os limites do consentimento*". Ele destaca a importância das chamadas *Privacy Enhancing Technologies* (PETs), tecnologias que aprimoram a privacidade em produtos e serviços. Alguns exemplos de PETs incluem padrões de criptografia, modelos de anonimização de dados pessoais e mecanismos de navegação anônima que evitam o rastreamento do usuário. Estas tecnologias são uma importante ferramenta para proteger a privacidade dos titulares de dados pessoais e são implementadas por meio de arquitetura de código.⁴²² Não obstante, deve haver um sopesamento das iniciativas citadas com as necessidades do Estado em relação a processos de investigação criminal, não devendo, em função da proteção à privacidade, fazer com que sua implementação prática facilite a prática de crimes cibernéticos, dificultando a identificação de indivíduos que cometem ilegalidades na rede mundial de computadores.⁴²³

Outro exemplo de PETs, a tecnologia DNT (*Do Not Track*) é desenvolvida para efetivar a decisão e os direitos do titular no momento da coleta dos seus dados. Bruno Bioni afirma que “ao contrário de fechar, rejeitar e/ou aceitar inúmeros *pop-ups* de *cookies* [...] basta o titular acionar o botão “DNT” para que, automaticamente, se exteriorize a sua escolha em barrar ou não a coleta de seus dados”.⁴²⁴ Isso já ocorre com alguns sistemas operacionais, como, por exemplo, a função “*App Tracking Transparency*”, da Apple, que requer do usuário uma autorização específica para cada aplicativo que deseja rastrear seus dados pessoais.⁴²⁵

⁴²¹ *ibid.*

⁴²² BIONI, 2018, *op. cit.*, p. 178.

⁴²³ DE GARCIA, Plínio Silva; MACADAR Marie Anne; LUCIANO, Edimara Mezzomo. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **Revista De Gestão Da Tecnologia E Sistemas De Informação**, v. 15, 2018.

⁴²⁴ BIONI, 2018, *op. cit.*, p. 180.

⁴²⁵ Mais informações em: <https://developer.apple.com/documentation/apptrackingtransparency>

Criado pelo *World Wide Web Consortium (W3C)*,⁴²⁶ o projeto P3P (*Platform for Privacy Preferences*)⁴²⁷ é outra abordagem ambiciosa de tecnologias PETs. Ele também pode ser visto como um modelo de arquitetura de código para proteção de dados pessoais. O P3P permite que navegadores, como o Microsoft Edge, Chrome, Firefox, entre outros, interajam com sites de forma a automaticamente ler e compreender as configurações de privacidade do usuário. Em resumo, o usuário define as restrições de coleta e tratamento de dados em seu navegador. Quando acessa um site ou serviço, este automaticamente reconhece as suas configurações, adaptando a coleta e tratamento de dados de acordo com as preferências do usuário, sem a necessidade de ler políticas de privacidade ou termos de consentimento. O próprio navegador verifica as políticas de privacidade do site e checa a compatibilidade com as preferências definidas pelo usuário.

Além de sua adoção em massa pelas organizações que desenvolvem *softwares*, navegadores e aplicações *web*, ambos os exemplos dependem, para a sua concretização, de um arcabouço regulatório que promova e estimule a adoção de padrões que permitam que tais tecnologias sejam operacionalizadas, possibilitando um aumento significativo do controle do titular sobre os seus dados pessoais, além de um importante estímulo e incentivo ao direito à autodeterminação informativa.⁴²⁸

Ainda que todas essas possibilidades tecnológicas e referenciais teóricos como o PbD apontem para a necessidade de interconexão entre o direito e a tecnologia, tais iniciativas não são novas. Nesse sentido, segundo Bruno Bioni:

O mantra de que serviços e produtos devem ser concebidos para garantir a privacidade tem sido repetido pelo menos desde a década 90, mas com pouca aderência prática. [...] Portanto, o PbD tem se mostrado um “conceito elusivo” e uma “promessa” ainda a ser

⁴²⁶ O World Wide Web Consortium (W3C) é uma comunidade internacional em que as organizações membros, uma equipe de tempo integral e o público trabalham juntos para desenvolver padrões da Web. Liderada pelo inventor e diretor da Web, Tim Berners-Lee, e pelo CEO Jeffrey Jaffe. Cf.: W3C. ABOUT W3C. Disponível em: <https://www.w3.org/Consortium/>. Acesso em 07 out. 2022.

⁴²⁷ O Projeto Plataforma para Preferências de Privacidade (P3P) permite que os sites expressem suas práticas de privacidade em um formato padrão que pode ser recuperado automaticamente e interpretado facilmente pelos navegadores do usuário. O P3P permite que os usuários sejam informados sobre as práticas do site (em formatos legíveis por máquina e humanos) e automatizem a tomada de decisões com base nessas práticas, quando apropriado. Portanto, os usuários não precisam ler as políticas de privacidade em todos os sites que visitam. Cf.: W3C. ABOUT W3C. Disponível em: <https://www.w3.org/Consortium/>. Acesso em 07 out. 2022.

⁴²⁸ BIONI, 2018, *op. cit.*, p. 185.

cumprida. Algo cuja gênese data da década de 80, esculpido especificamente na década de 90, mas que mesmo já em 2019 ainda não decolou. Ao olhar no retrovisor e reconstruir a linha do tempo da formação do conceito de PbD, não há muito o que se comemorar e, em última análise, é duvidosa o quão efetiva é a estratégia de leis que positivaram ou prescreveram o seu conceito.⁴²⁹

O autor acrescenta que os principais desafios para a implementação do conceito de PbD não tem qualquer relação com sua falta de previsão em lei. Trata-se, no entanto, da ausência de um maior debate entre reguladores e regulados, especialmente com aqueles responsáveis pelo desenvolvimento de sistemas de tecnologia de informação, além da ausência de um mercado mais desenvolvido de soluções tecnológicas para a melhoria de proteção de dados pessoais, com eventuais incentivos econômicos para que haja a concepção de produtos e serviços utilizadores dessas soluções.⁴³⁰

Portanto, a própria LGPD traz o caminho que deve ser perseguido por organizações públicas e privadas para que os riscos derivados de suas operações sejam, de alguma forma, mitigados. Seja pela adoção de ferramentas de mitigação de riscos, programas de governança e *compliance*, ou a consideração dos princípios do PbD, são inúmeros os caminhos que podem ser trilhados para uma efetiva tutela da privacidade e redução dos “efeitos colaterais” do tratamento de dados no Brasil. Todavia, para que a adoção dessas ferramentas se concretize, é fundamental que haja comandos regulatórios nesse sentido. A Autoridade Nacional de Proteção de Dados assume, assim, um papel essencial para a promoção da tutela da privacidade e proteção de dados pessoais.

3.6. O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS PARA A TUTELA DA PRIVACIDADE

⁴²⁹ BIONI, Bruno Ricardo. Abrindo a “caixa de ferramentas” da LGPD para dar vida ao conceito ainda elusivo de *privacy by design*. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019. P. 242.

⁴³⁰ BIONI, Bruno Ricardo. Abrindo a “caixa de ferramentas” da LGPD para dar vida ao conceito ainda elusivo de *privacy by design*. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019. P. 253.

Como meio de intensa manifestação social, a tecnologia e a Internet são grandes responsáveis pela viabilização do novo modelo de sociedade baseado em dados pessoais, na qual a tecnologia da informação é uma ferramenta indispensável para a construção de conhecimento e para a dinâmica da economia.⁴³¹

Assim, ao utilizar serviços e produtos, os titulares fornecem seus dados pessoais, que acabam sendo utilizados para uma série de finalidades. Isso aumenta, conseqüentemente, a lucratividade das empresas que fazem uso dessas informações. Como efeito, isso gera a necessidade do Estado regular o ambiente digital.⁴³² Não obstante, deve-se ter a consciência de que “a angústia do futuro não implica a recusa do futuro”⁴³³, ou seja, diante da impossibilidade de deter o progresso tecnológico, é necessário um alargamento da perspectiva institucional de proteção à pessoa humana, integrando controles individuais e coletivos.⁴³⁴

Não se trata de proibir as tecnologias ou paralisar a inovação, mas que haja instrumentos e mecanismos adequados para que decorra a expansão da ciência, da tecnologia e da indústria, conduzida de forma a considerar parâmetros razoáveis de segurança.⁴³⁵

Na União Europeia, por exemplo, os avanços econômicos e tecnológicos da década de 70 promoveram uma série de legislações nacionais de proteção de dados para regular o tratamento de dados pessoais, que posteriormente seriam unificadas pela Diretiva 95/46/CE e, mais recentemente, pelo RGPD.⁴³⁶ Conforme já analisado, com a intensificação do tratamento de dados pessoais pelos Estados e por grandes conglomerados multinacionais, o direito fundamental à privacidade deixou de ser meramente um direito à vida íntima do indivíduo. Agora, ele passa para um contexto muito mais amplo de controle dos dados pessoais e autodeterminação informativa.⁴³⁷

⁴³¹ CASTELLS, *op. cit.*, pp. 67-69.

⁴³² CAVEDON; FERREIRA; FREITAS, *op. cit.*, 2015.

⁴³³ RODOTÁ, *op. cit.*, p. 41.

⁴³⁴ RODOTÁ, *op. cit.*, p. 50.

⁴³⁵ FERREIRA, 2008, *op. cit.* p. 42.

⁴³⁶ RUDGARD, Sian; et al. **European Data Protection: Law and Practice**. Portsmouth: Jeanne R. Busemeyer, Hide Park Publishing Services. p. 21-52, 2018.

⁴³⁷ SCHEREIBER, *op. cit.*, pp. 138-140.

Surge, a partir disso, o recurso de criação de autoridades administrativas para a proteção de dados pessoais, no modelo de autoridades independentes. Essas autoridades podem ser definidas, segundo Danilo Doneda, como:

[...] entes ou órgãos públicos dotados de substancial independência do governo, caracterizados pela sua autonomia de organização, financiamento e contabilidade; da falta de controle e sujeição ao poder executivo, dotadas de garantias de autonomia através da nomeação de seus membros, dos requisitos para esta nomeação e da duração de seus mandatos; e tendo a função de tutela de interesses constitucionais em campos socialmente relevantes.⁴³⁸

No Brasil, a ANPD é a entidade responsável pela aplicação, fiscalização e regulamentação da LGPD. Criada pela Lei nº 13.853/19, oriunda da Medida Provisória nº 869/18, a ANPD foi instituída para zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade e para aplicar sanções em casos de tratamento de dados feitos de forma irregular, dentre outras atribuições dispostas na lei.

A estrutura organizacional da ANPD é dividida em (artigo 55-C, LGPD): (i) Conselho Diretor; (ii) Conselho Nacional de Proteção de Dados Pessoais e Privacidade; (iii) Corregedoria; (iv) Ouvidoria; (v) Órgão de assessoramento jurídico próprio e (vi) Unidades administrativas e especializadas necessárias para a aplicação das diretrizes da lei.

Conforme dispõe o *caput* do artigo 55-A da referida legislação, após passar por um período de transição vinculada à Presidência da República, atualmente a ANPD assume a característica de autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

A atuação da ANPD, assim como outras autoridades do tipo no mundo, tem como principal motivação a necessidade de proteção dos interesses dos titulares de dados. Trata-se de uma evolução do direito fundamental à proteção de dados, no sentido da constatação de que os titulares, individualmente, têm pouca ou nenhuma capacidade de projetar um controle ou tutela sobre os direitos fundamentais envolvidos. Danilo Doneda afirma que:

A impossibilidade de concretizar a autodeterminação informativa baseada meramente na ação singular de seu interessado é patente em vista de diversos fatores, como a crescente complexidade dos

⁴³⁸ DONEDA, 2019, *op. cit.*, p. 324.

mecanismos de tratamento de dados e a dificuldade em se estabelecer nexos causais entre este tratamento e os efeitos por ele causados à pessoa, ou a desproporção entre sua vontade autônoma e uma estrutura dirigida à coleta de seus dados preparada a excluí-lo de certas vantagens caso decida por não fornecê-los.⁴³⁹

Portanto, a tutela singular, exercida individualmente, é insuficiente e compreende, ainda segundo o autor, uma “tradição elitista da privacidade”⁴⁴⁰, que não corresponde ao nível constitucional dos direitos tutelados, seja no âmbito da personalidade, como também em relação à igualdade e liberdades individuais.

A missão institucional da ANPD une, portanto, a proteção aos direitos fundamentais dos titulares de dados, além dos desafios de regular diversos setores da economia, estimulando a adoção de padrões que facilitem o exercício e o controle dos dados pessoais pelos titulares, conforme previsão do artigo 55-J, VIII, da LGPD.

Cabe, portanto, à ANPD, estimular e movimentar o mercado para a adoção de padrões a serem adotados, visto que a LGPD, acertadamente, não especifica quais são essas medidas técnicas a serem adotadas, evitando, assim, que estas rapidamente se tornem obsoletas como consequência das evoluções tecnológicas e mudanças técnicas características da Sociedade Informacional.⁴⁴¹ Não obstante, conforme analisado no tópico 3.5, existem grandes oportunidades em utilizar o modelo de regulação pela arquitetura, ou seja, de regular o modo como o código (programa de computador ou *software*) deve ser desenvolvido, levando em consideração os princípios, regras e boas-práticas em proteção de dados pessoais.

Nesse cenário, é papel da ANPD pensar em modelos regulatórios e fiscalizatórios tanto para o setor privado quanto para o setor público, uma vez que, dada a amplitude do conceito de tratamento de dados,⁴⁴² tais operações ocorrem independentemente do agente econômico envolvido, ao contrário das agências reguladoras brasileiras, que possuem sua atuação restrita à um setor

⁴³⁹ DONEDA, 2019, *op. cit.*, p. 333.

⁴⁴⁰ DONEDA, 2019, *op. cit.*, p. 334.

⁴⁴¹ LEMOS; BRANCO, *op. cit.*, p. 450.

⁴⁴² O art. 5º, inciso X, da Lei Geral de Proteção de Dados define tratamento de dados pessoais: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

específico – como é o caso da Agência Nacional de Telecomunicações (Anatel), Agência Nacional de Energia Elétrica (Aneel), dentre outros exemplos.⁴⁴³

Apesar da relevância do tema, não há menção expressa a um desenvolvimento de um modelo de regulação por arquitetura no planejamento estratégico da ANPD. O atual documento, que compreende o planejamento da autoridade entre os anos de 2021 e 2023, estabelece três objetivos estratégicos da autoridade.⁴⁴⁴

O primeiro, institui como prioridade a promoção do “fortalecimento da cultura de Proteção de Dados Pessoais”⁴⁴⁵ por meio de eventos de capacitação, oficinas, diálogos com entidades governamentais e não-governamentais e elaboração de guias e recomendações sobre proteção de dados, como o “*Guia orientativo para definição dos Agentes de Tratamento de Dados Pessoais e do Encarregado*”⁴⁴⁶, o “*Guia orientativo de Segurança da Informação para agentes de tratamento de pequeno porte*”⁴⁴⁷, entre outros disponíveis no sítio da ANPD.⁴⁴⁸

O segundo objetivo estratégico da autoridade é o de “Estabelecer ambiente normativo eficaz para a Proteção de Dados Pessoais”⁴⁴⁹. Entre as ações dessa meta, estão a análise de comunicados de incidentes de segurança

⁴⁴³ ALMEIDA, R. Oliveira Reis; SAIKALI, L. Bossoni; ALMENDRA FREITAS, Cinthia Obladen de. Políticas regulatórias para a proteção de dados no Brasil e a aplicabilidade do modelo de regulação pela arquitetura de código ou privacy by design. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 16, n. 46, p. 363–385, 2022. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1118>. Acesso em: 02 dez. 2022.

⁴⁴⁴ BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

⁴⁴⁵ BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

⁴⁴⁶ BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 02 dez. 2022.

⁴⁴⁷ BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 02 dez. 2022.

⁴⁴⁸ BRASIL. Autoridade Nacional de Proteção de Dados. **Publicações da ANPD**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 02 dez. 2022.

⁴⁴⁹ BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/aceso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

e petições de titulares para que haja uma contínua avaliação entre as demandas concluídas e o recebimento de reclamações.

Por fim, o terceiro objetivo é o aprimoramento das “condições para o cumprimento das competências legais”,⁴⁵⁰ que se relaciona com a estruturação do corpo técnico da autoridade, questões orçamentarias e de infraestrutura da informação.⁴⁵¹

Portanto, partindo da análise dos atuais objetivos estratégicos, é crucial que haja clareza na criação de políticas regulatórias pela ANPD, vez que cabe à autoridade levar em consideração os interesses envolvidos e traçar estratégias e políticas regulatórias efetivas⁴⁵², visando, especialmente, a adoção de padrões tecnológicos, metodologias de mitigação de risco e boas-práticas no tratamento de dados pessoais.

⁴⁵⁰ BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

⁴⁵¹ BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

⁴⁵² ALMEIDA; SAIKALI; ALMENDRA FREITAS, *op. cit.*, p. 277.

CONCLUSÃO

A Sociedade Informacional, tal como concebida por Manuel Castells, vêm se mostrando um colosso do desenvolvimento econômico, especialmente nos ambientes onde as gigantes da tecnologia se instalaram, como, por exemplo, a região do Vale do Silício, Nova Iorque e Shanghai.⁴⁵³ São inquestionáveis, igualmente, os avanços em diversas áreas do conhecimento. Em pouco mais de 50 anos, décadas de um composto imaginário de cineastas de ficção científica se tornaram tecnologias corriqueiras no nosso cotidiano. Ligações por videoconferência, dispositivos inteligentes e carros autônomos se tornaram possíveis, principalmente, com o advento da Internet, de tecnologias de transmissão de dados em alta velocidade e de técnicas em IA e *Big Data*. São avanços que permitiram não só o desenvolvimento da sociedade, mas, também, a potencialização do próprio ser humano em suas capacidades físicas e mentais por meio do desenvolvimento de disciplinas como a biotecnologia, biomedicina, robótica e as diversas aplicações do campo da inteligência artificial para aumento da capacidade cognitiva e analítica do ser humano.

O surgimento da Sociedade Informacional criou as condições necessárias para esse progresso sem precedentes na história, que culmina num repensar do sistema clássico de acumulação de riquezas baseado nos meios de produção e na criação de uma sociedade convergente, consistindo na intercomunicação de coisas e pessoas por meio de uma conexão constante. Vivemos uma era de conectividade, de encurtamento de distâncias, de aumento da eficiência e proliferação de soluções para praticamente todos os problemas da humanidade – para isso, basta fornecer seus dados pessoais.

Em 2006, a matemática britânica Clive Humby cunhou um termo que seria vastamente utilizado em artigos e trabalhos acadêmicos – *“data is the new oil”*⁴⁵⁴. Hoje, apesar da assertividade da afirmação à época, pode-se dizer que a verdadeira “mina de ouro” do século XXI não são os dados propriamente ditos,

⁴⁵³ BATEMAN, Kayleigh. Which are the world's most innovative cities in 2022? In: **World Economic Forum**, 2022. Disponível em: <https://www.weforum.org/agenda/2022/02/innovative-global-cities-talent-property/>. Acesso em: 02 dez. 2022.

⁴⁵⁴ Em tradução livre: Dados são o novo petróleo. Cf.: THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**. 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 02 fev. 2023.f

mas a capacidade de cada organização processá-los de forma a extrair novos *insights* e informações que agreguem valor às informações. Trata-se, portanto, de um produto de luxo, cuidadosamente extraído dos imensuráveis rastros digitais deixados por desavisados indivíduos, que, entorpecidos pela magia da tecnologia, pouco notam as consequências do seu uso.

Assim, presencia-se uma realidade marcada pelo vertiginoso aumento dos riscos provocados pelo modo como as TICs passam a permeabilizar a vida em sociedade. A modernização acelerada associa a produção de bens e serviços com a produção sistemática de riscos, que agora são o efeito colateral inevitável do progresso tecnológico e econômico.

Os riscos, então, saem das fábricas e usinas nucleares e passam a compor os serviços oferecidos por milhares de organizações públicas e privadas, que tratam dados pessoais em escala cada vez maior, mudando substancialmente as suas características. Nesse sentido, eles se tornam mais complexos, mais globalizados, mais catastróficos e menos perceptíveis.

Diante desse cenário de produção sistemática de riscos em uma sociedade hiperconectada, buscou-se analisar de que forma as TICs, no contexto da Sociedade Informacional, contribuem para a configuração da Sociedade de Risco proposta pelo sociólogo Ulrich Beck.

Para isso, o presente trabalho analisou as transformações sociais ocasionadas pela revolução das Tecnologias da Informação e Comunicação, que alteraram a lógica de funcionamento da sociedade industrial clássica por meio de um processo de retroalimentação de conhecimento agindo sobre o conhecimento. Essa lógica caracterizou a revolução tecnológica do último século, gerando um ciclo de convergência e inovação de inúmeras tecnologias em microeletrônica, computação, *softwares*, entre outros. Houve, a partir disso, um deslocamento do capitalismo tradicional para uma economia movida a dados e conhecimento, com serviços de alto valor agregado e cujo produto é, essencialmente, imaterial. Essa revolução tecnológica culmina no que Manuel Castells chama de Sociedade Informacional, um novo sistema sociotécnico com características totalmente diferentes da Sociedade Industrial clássica.

Nesse ponto, passou-se a desenvolver o conceito de modernidade reflexiva, conforme proposto por Ulrich Beck, que retrata um momento da modernidade em que, em função do próprio progresso e das vitórias do

capitalismo, passa por um processo de autodestruição contínuo e silencioso. Dessa forma, a modernidade reflexiva representa a passagem da Sociedade Industrial clássica para a Sociedade de Risco, que ocorre conforme se intensifica a produção sistemática de riscos no corpo social. Esse processo gera uma disfuncionalidade na sociedade que a torna irracional em relação aos perigos produzidos por ela mesma. A Sociedade de Risco, portanto, caracteriza-se pelo modo como os perigos criados pelo progresso transcendem limites temporais e espaciais, de modo que passam a afetar o ser humano em uma escala global, bem como as futuras gerações.

Para compreender de que forma a hiperconectividade impacta a criação de riscos na Sociedade Informacional, verificou-se que o advento da Internet, e, posteriormente, das técnicas de IA e do uso do *Big Data*, foram determinantes para que fosse confirmada a hipótese do presente trabalho, qual seja, a da existência de uma dimensão digital da Sociedade de Risco. O contexto da Sociedade Informacional é marcado pela popularização das plataformas e mídias sociais que lucram com a utilização irrefreada de dados pessoais dos seus usuários. Cria-se, nesse cenário, um novo modelo do capitalismo informacional que visa antecipar e modificar o comportamento humano com finalidades puramente mercadológicas. Isso provoca inúmeros riscos ao livre desenvolvimento da personalidade, conforme algoritmos passam a filtrar nossa comunicação e nos inserir em bolhas de pessoas parecidas entre si.

Não obstante, o *Big Data*, em conjunto com técnicas de IA, passa a modular o comportamento humano, controlando a visualização de conteúdos na Internet e induzindo indivíduos a determinados comportamentos mais vantajosos aos interesses das organizações, com o objetivo de reter a atenção e a influenciar as decisões de compra de consumidores. Isso, entre outras consequências, acaba por alterar a percepção de mundo dos indivíduos, refletindo suas escolhas e instaurando um regime de vigilância com potenciais catastróficos, seja no aspecto individual – com a deterioração completa da privacidade, ou no espectro coletivo, com perigosas consequências ao Estado Democrático de Direito em consequência das manipulações eleitorais por meio da disseminação em massa das *Fake News*.

Diante desse panorama, passou-se a comparar os elementos caracterizadores da Sociedade de Risco, conforme originalmente concebido por

Ulrick Beck, com as características próprias da utilização de TICs em uma Sociedade Informacional hiperconectada e os riscos gerados por elas. Evidenciou-se que o processo de modernização reflexiva descrita pelo sociólogo alemão se adere perfeitamente aos riscos e à privacidade ocasionados pelo uso das TICs no contexto da Sociedade Informacional, fazendo com que um turbilhão de novos e complexos riscos se mostrem imprevisíveis e incontroláveis. Estes, embora não afetem o meio ambiente, podem transformar os dados pessoais dos indivíduos em mera mercadoria, reduzindo a personalidade humana a um mero objeto.

Esse paradigma emergente, pautado na dicotomia entre os interesses econômicos advindos do uso de dados pessoais e os impactos em direitos e liberdades fundamentais dos indivíduos, provoca intensos reflexos no Direito. Parte-se, então, para a análise da evolução do conceito de privacidade, que passa a ser entendido, modernamente, como o direito de manter o controle sobre os próprios dados pessoais. No contexto brasileiro, examina-se a Emenda Constitucional nº 115 de 2022, que elegeu a proteção de dados pessoais ao rol de direitos e garantias fundamentais. Em consequente, explora-se o regime de proteção de dados pessoais no Brasil que, apesar da sua coexistência com outras legislações, é liderado pela Lei Geral de Proteção de Dados.

Passa-se, então, a relacionar os riscos caracterizados pela Sociedade Informacional hiperconectada com os instrumentos e previsões pertinentes sobre o tema presentes na LGPD. Conclui-se, nesse aspecto, que a referida lei, assim como outras legislações internacionais, prescreve a forma como o controlador ou o operador de dados deve agir para que haja uma efetiva redução de riscos no tratamento de dados pessoais por organizações públicas ou privadas. Desde a década de 1980, processos de gestão de risco desempenham um papel cada vez mais importante para garantir a conformidade das organizações com as leis de proteção de dados, bem como proteger os direitos fundamentais e liberdades dos titulares de dados.

Há, desse modo, uma abordagem baseada em riscos para a proteção de dados pessoais em legislações como a LGPD, com diversos comandos normativos que, mais do que encorajar, recomendam às organizações controladoras e operadoras de dados a implementação de medidas de proteção compatíveis com o nível de risco de suas atividades de tratamento. Se torna

essencial a compreensão das ferramentas que permitem a análise e gerenciamento de riscos nas organizações. Constatase, assim, que a adoção de padrões normativos, investimentos em gestão de risco, segurança da informação e ferramentas de *compliance*, podem auxiliar as organizações na adoção de medidas de mitigação de risco, especialmente em contextos em que o tratamento de dados possa ocasionar graves danos aos titulares de dados pessoais.

Chega-se, então, ao modelo *Privacy by Design*, conceito criado a partir de sete princípios que visam articular a proteção de dados para além de comandos legais, inserindo os conceitos de privacidade na concepção de produtos e serviços que tratam dados pessoais. Embora não se pretenda elencar o modelo como uma solução definitiva para os riscos da Sociedade Informacional, propõe-se que a regulação pela arquitetura de códigos possa ser um modelo de regulação mais eficiente que a própria lei, limitando potenciais tratamentos de dados pessoais em desacordo com os princípios e normas de proteção de dados.

Por fim, traz-se como contribuição o apontamento de alguns caminhos possíveis para que as organizações públicas e privadas, controladoras e operadoras de dados pessoais, reduzam os riscos relacionados à sua operação, utilizando processos e ferramentas de gerenciamento de risco e *compliance* que devem ser estimulados por meio de uma regulação pela arquitetura de códigos. Para que isso ocorra, é fundamental que haja comandos regulatórios no sentido da adoção de padrões no desenvolvimento de *softwares*, serviços e produtos que levem em consideração os princípios, regras e boas práticas em proteção de dados pessoais desde a sua concepção, contribuindo para um maior controle dos riscos criados pelas TICs em uma Sociedade Informacional hiperconectada.

REFERÊNCIAS

- AGUIAR, Rodrigo Goulart. **Sociedade em rede e internet: direitos fundamentais em diálogo**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, 2015.
- ALMEIDA, R. Oliveira Reis; SAIKALI, L. Bossoni; ALMENDRA FREITAS, Cinthia Obladen de. Políticas regulatórias para a proteção de dados no Brasil e a aplicabilidade do modelo de regulação pela arquitetura de código ou privacy by design. **Revista Brasileira de Direitos Fundamentais & Justiça**, [S. l.], v. 16, n. 46, p. 363–385, 2022. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/1118>. Acesso em: 02 dez. 2022.
- SILVEIRA, S. Amadeu da. A noção de modulação e os sistemas algorítmicos. **PAULUS: Revista de Comunicação da FAPCOM**, [S. l.], v. 3, n. 6, 2019. Disponível em: <https://fapcom.edu.br/revista/index.php/revista-paulus/article/view/111>. Acesso em: 22 nov. 2022.
- ARAYA, Erm.; VIDOTTI, Sabg. **Criação, proteção e uso legal de informação em ambientes da World Wide Web [online]**. São Paulo: Editora UNESP; São Paulo: Cultura Acadêmica, 2010.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013: **Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, 2013.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27005:2019: **Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro, 2019a.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701:2019: **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Rio de Janeiro, 2019b.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31.000:2018: **Gestão de Riscos — Diretrizes**. Rio de Janeiro, 2018.
- BARLOW, John Perry. A Declaration of the Independence of Cyberspace. In: **Electronic Frontier Foundation**, 1996. Disponível em: <https://www.eff.org/pt-br/cyberspace-independence>. Acesso em: 02 dez. 2022.
- BATEMAN, Kayleigh. Which are the world's most innovative cities in 2022? In: **World Economic Forum**, 2022. Disponível em: <https://www.weforum.org/agenda/2022/02/innovative-global-cities-talent-property/>. Acesso em: 02 dez. 2022.

- BAUMAN, Zygmunt. **Modernidade líquida**. Trad. Plínio Dentzien. Rio de Janeiro: Zahar, 2001.
- BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.
- BECK, Ulrich. **La sociedad del riesgo global**. España: Siglo Veintiuno, 2002.
- BECK, Ulrich. **Sociedade de risco: rumo a uma outra modernidade**. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2011.
- BECK, Ulrich. **Sociedade global de risco: em busca da segurança perdida**. São Paulo: Editora 70, 2015.
- BECK, Ulrich; GIDDENS, Anthony; LASH, Scott. **Modernização reflexiva: política, tradição e estética na ordem social moderna**. São Paulo: Editora da Universidade Estadual Paulista, 1997.
- BIONI, Bruno Ricardo. Abrindo a “caixa de ferramentas” da LGPD para dar vida ao conceito ainda elusivo de privacy by design. In: **Direito e Internet IV: Marco Civil da Internet - 5 anos, GDPR e LGPD, inteligência artificial e direitos fundamentais**. São Paulo: Thomson Reuters Brasil, 2019.
- BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.
- BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a proteção de dados pessoais no ciberespaço como um direito fundamental: perspectivas de construção de um marco regulatório para o Brasil**. Revista Eletrônica do Curso de Direito da UFSM, Santa Maria, v. 11, n. 1, p. 258-277, 2016.
- BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de Dados e Privacidade: Do direito às novas tecnologias na Sociedade Informacional**. Rio de Janeiro: Lúmen, 2018.
- BRASIL. **Constituição da República Federativa do Brasil, 1988**. Brasília-DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 28 mar. 2022.
- BRASIL. **Lei 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília-DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em 13 nov. 2022.
- BRASIL. **Lei 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e

no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília-DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 13 nov. 2022.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília-DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13. jun. 2022.

BRASIL. **Lei 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/L13709.htm. Acesso em: 12 dez. 2022.

BRASIL. **Lei 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/l8078compilado.htm. Acesso em: 13 nov. 2022.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Segurança e Proteção de Dados – Guias e modelos**. 2021. Disponível em: <https://www.gov.br/gestao/pt-br>. Acesso em: 13 nov. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Acesso em: 02 dez. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Planejamento Estratégico 2021-2023**. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/planejamento-estrategico-anpd-versao-2-0-06072022.pdf>. Acesso em: 02 dez. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Publicações da ANPD**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em: 02 dez. 2022.

CAPPA, F.; FRANCO, S.; ROSSO, F. Citizens and cities: Leveraging citizen science and bigdata for sustainable urban development. **Business Strategy and the Environment**, v. 31, n. 2, p. 648–667, 2022.

CARTURAN, Sara B. O. G.; MATSUI, Beatriz M. A.; GOYA, Denise H.. GPD Framework: An Implementation and *Compliance* Guide for Technology Areas. **[Anais...]** XLIX Seminário Integrado de Software e Hardware, p. 176-187, 2022.

Disponível em:

<https://sol.sbc.org.br/index.php/semish/article/view/20807/20633>. Acesso em: 02 fev. 2023.

CARVALHO, Vinicius Marques de; MATTIUZZO, Marcela; PONCE, Paula Pedigoni. Boas práticas e governança na LGPD. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021.

CASSINO, João Francisco. Modulação deleuziana, modulação algorítmica e manipulação midiática. In: **Sociedade de Controle: Manipulação e modulação nas redes digitais**. 1. ed. São Paulo, SP. Hedra, 2018.

CASTELLS, Manuel. **A Sociedade em Rede**. Tradução Roneide Venancio Majer, 22. ed. São Paulo: Paz e Terra, 2020.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. A dimensão ambiental da teoria da Sociedade de Risco. In: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). **Direito Socioambiental e Sustentabilidade: Estados, Sociedades e Meio Ambiente**. Curitiba: Letra da Lei, 2016.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. O meio ambiente digital sob a ótica da teoria da sociedade de risco: os avanços da informática em debate. **Revista Direito Ambiental e Sociedade**, v. 5, p. 194-223, 2015.

CAVOUKIAN, Ann. Privacy by design: The 7 foundational principles. **Information and Privacy Commissioner of Ontario**, Canada, v. 5, 2009.

CIPL. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. CIPL GDPR Interpretation and Implementation Project, 2016.

CNIL. **Measures For The Privacy Risk Treatment**. 2012a.

CNIL. **Methodology For Privacy Risk Management: How to implement the Data Protection Act**. 2012b.

CNIL. (2015). **Privacy Impact Assessment (PIA): Methodology (how to carry out a PIA)**. Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>. Acesso em: 12 dez. 2022.

CONCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. Disponível em: <https://rm.coe.int/1680078b37>. Acesso em: 12 dez. 2022.

CUKIER, Kenneth; MAYER-SCHOENBERGER, Viktor. The Rise of Big Data: How It's Changing the Way We Think About the World. **Foreign Affairs**, v. 92, n. 3, p. 28-40, 2013. Disponível em: <http://www.jstor.org/stable/23526834>. Acesso em: 12 dez. 2022.

DAVENPORT, T. H. **Ecologia da informação**: porque só a tecnologia não basta para o sucesso na era da informação. Tradução B. S. Abrão. São Paulo: Futura, 1988.

DE GARCIA, Plinio Silva; MACADAR Marie Anne; LUCIANO, Edimara Mezzomo. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **Revista De Gestão Da Tecnologia E Sistemas De Informação**, v. 15, 2018.

DE MARCO, Cristhian Magnus; DE CASTRO, Matheus Felipe. As dimensões e perspectivas do direito fundamental ao livre desenvolvimento da personalidade. **Revista Prisma Jurídico**, v. 12, n. 1, 2013. Disponível em: <https://periodicos.uninove.br/prisma/article/view/4253/2530>. Acesso em: 12 dez. 2022.

DE SOUZA, Clarisse S. **Vida na Era da Hiperconectividade**. EMAPS-Resenhas #05. Rio de Janeiro, RJ - Brasil: SERG, Departamento de Informática, PUC-Rio, 2021. p. 15. Disponível em: <http://www.hcc.inf.puc-rio.br/EMAPS/userfiles/downloads/Resenha-Floridi2015.pdf>. Acesso em: 6 nov. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters, 2019.

DONEDA, Danilo. Panorama histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DOWBOR, Ladislau. **O capitalismo se desloca**: novas arquiteturas sociais. São Paulo: Edições Sesc-SP, 2020.

DIMITROPOULOU, Alexandra. Economy Rankings: Largest countries by GDP, 2022. In: **CeoWorld Magazine**, 2022. Disponível em: <https://ceoworld.biz/2022/03/31/economy-rankings-largest-countries-by-gdp-2022/#:~:text=World%20GDP%3A%20The%20World%27s%20GDP,countries%20from%202019%20to%202026>. Acesso em: 21 out. 2022.

DYSON, Esther. **Reflexões sobre privacidade**. Scientific American Brasil, [S.l.], n. 77, p.1-12, 01 out. 2008.

ESPON. Using big data for policy-making in the public interest. In: **ESPON BLOG**, 2020. Disponível em: <https://www.espon.eu/using-big-data-policy-making-public-interest>. Acesso em: 15 nov. 2022.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 apr. 2016**. Disponível em: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 15 nov. 2022.

FERNANDAS, Jorge Henrique Cabral. **Introdução à gestão de riscos de segurança da informação.** >> Gestão da Segurança da Informação e Comunicações >> 2009-2011. GSIC302. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC302_Introducao_Gestao_Riscos_Seguranca_Informacao.pdf. Acesso em: 02 fev. 2023.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. Privacidade e proteção de dados pessoais: perspectiva histórica. **InCID: Revista de Ciência da Informação e Documentação**, Ribeirão Preto, v. 12, n. 2, p. 151-172, set. 2021./fev. 2022.

FERREIRA, Heline Sivini. **A biossegurança dos organismos transgênicos no direito ambiental brasileiro:** uma análise fundamentada na teoria da sociedade de risco. Tese (Doutorado em Direito) – Universidade Federal de Santa Catarina, CPGD, 2008.

FERREIRA, Heline Sivini. A dimensão ambiental da teoria da sociedade de risco. In: FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra (orgs.). **Direito Socioambiental e Sustentabilidade:** Estados, Sociedades e Meio Ambiente. Curitiba: Letra da Lei, 2016.

FONTANEL, Jacques. GAFAM, a progress and a danger for civilization. Financial Architecture; **Forced Economic Development ion the Context of External Shocks and Internal Inconsistencies**, St. Peters-burg State University of Economics (UNECON), Apr 2019, Saint-Petersbourg, Russia. hal-02102188

FORGÓ, N., HÄNOLD, S., SCHÜTZE, B. The Principle of Purpose Limitation and Big Data. In: Corrales, M., Fenwick, M., Forgó, N. (eds) **New Technology, Big Data and the Law. Perspectives in Law, Business and Innovation**, Springer, Singapore, 2017. p. 18. ISBN 978-981-10-7055-5.

FREITAS, Cinthia Obladen de Almendra. Tratamento de dados pessoais e a legislação brasileira frente ao profiling e à discriminação a partir das novas tecnologias. **Revista de Direito, Governança e Novas Tecnologias**, v. 3, n. 2, ju./dez. 2017.

FREITAS, Cinthia Obladen de Almendra; BARDDAL, Jean Paul. Análise preditiva e decisões judiciais: controvérsia ou realidade? **Democracia Digital e Governo Eletrônico**, v. 1, p.107-126, 2019.

FREITAS, Cinthia Obladen de Almendra; FERREIRA, Heline Sivini; CAVEDON, Ricardo. A bolha informacional e os riscos dos mecanismos de busca na personalização do usuário de internet: reflexões sobre o direito à autodeterminação informacional. **Revista Brasileira de Direito**, Passo Fundo, vol. 16, n. 3, p. 1-24, set./dez. 2020.

FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. **A segurança da informação como ferramental técnico da proteção de dados pessoais**. Direito e Inovação v. 3. Curitiba: OAB/PR, 2020.

FREITAS; Cinthia Obladen de Almendra; BARDDAL, Jean Paul. Análise preditiva e decisões judiciais: controvérsia ou realidade? **Democracia Digital e Governo Eletrônico**, v. 1, p. 107-126. 2019.

FREITAS; Cinthia Obladen de Almendra; FERREIRA, Heline Sivini; CAVEDON, Ricardo. Reflexões sobre o direito à autodeterminação informacional a partir das bolhas informacionais e dos riscos associados aos mecanismos de busca diante da personalização do usuário de internet. In: NETO, José Querino Tavares; FREITAS, Cinthia Obladen de Almeida; COSTA, Andréa Abrahão. **Métodos e pesquisas avançadas em direito**. Curitiba: CRV, 2021.

GELLERT, R. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. **International Data Privacy Law**, v. 5, n. 1, p. 3-19, 2015.

GELLERT, Raphael. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, [S.l.], v. 33, n. 1, p. 12-23, 2017. Disponível em: <https://doi.org/10.1016/j.clsr.2016.11.007>. Acesso em: 27 nov. 2022.

Global Commission on Internet Governance. Disponível em: <https://ourinternet.org/>. Acesso em: 20 out. 2022.

HAN, Byung-Chul. **Infocracia: Digitalização e a crise da democracia**. 1. ed. Petrópolis: Editora Vozes, 2022.

HAN, Byung-Chul. **Sociedade da transparência**. 1. ed. Petrópolis: Editora Vozes, 2016.

HAN, Jiawei; PEI, Jian; KAMBER, Micheline. Data Mining. **The Morgan Kaufmann Series in Data Management Systems**. Saint Louis: Elsevier Science & Technology, 2011

HENRIQUE NETO, Sylvio. **Democracia e tecnologia da informação: o tríplice conflito entre criptografia, vigilância e privacidade nos Estados Unidos**. 2019. Tese (Doutorado em Ciência Política) – Faculdade de Filosofia, Letras e Ciências Humanas, Universidade de São Paulo, São Paulo, 2019. Acesso em: 02 fev. 2023.

HENRIQUES, Isabella; PITA, Mariana; HARTUNG, Pedro. A proteção de dados pessoais de crianças e adolescentes. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021.

HUXLEY, Aldous. **Admirável mundo novo**. Tradução Lino Vallandro e Vidal Serrano. 22. ed. São Paulo: Globo, 2014.

INFORMATION COMMISSIONER'S OFFICE. **Big data, artificial intelligence, Machine Learning and data protection**. Disponível em: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. Acesso em: 15 nov. 2021.

LANA, Alice de Perdigão; D'ALMEIDA, Érica Nogueira Soares. A efetividade da solução do consentimento na proteção de dados pessoais. In: PEREIRA, Alexandre Libório Dias; WACHOWICZ, Marcos; LANA, Pedro de Perdigão. (coord.) **Novos direitos intelectuais: estudos luso-brasileiros sobre propriedade intelectual, inovação e tecnologia**. Curitiba: Gedai, 2019.

LARICCHIA, Federica. Leading tech companies worldwide 2022, by market capitalization. In: **Technology & Telecommunications**, 2023. Disponível em: <https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/>. Acesso em: 02 fev. 2023.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. Rio de Janeiro: Livros Técnicos e Científicos S.A., 1999.

LEMONS, Ronaldo; BRANCO, Sérgio. Privacy by Design: conceito, fundamentos e aplicabilidade na LGPD. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES, Otavio Luiz; BIONI, Bruno (Coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Forense, 2021.

LEONARDI, Marcel. **Publicidade Personalizada e LGPD**. 2021. Disponível em: <https://iabbrasil.com.br/publicacoes/parecer-juridico-lgpd-e-publicidade-personalizada/>. Acesso em: 23 out. 2021.

LEONARDI, Marcel. Transferência Internacional de Dados. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021.

LEONARDI, Marcel. **Tutela da privacidade na internet**. São Paulo: Saraiva, 2011.

LESSIG, Lawrence. **Code: and other laws of cyberspace**. New York: Basic Books, 2006.

LIMA, E. C. DE; OLIVEIRA NETO, C. R. DE. Revolução Industrial: considerações sobre o pioneirismo industrial inglês. **Revista Espaço Acadêmico**, v. 17, n. 194, p. 102-113, 6 jul. 2017.

LITTLE, Josh. Risk in the age of information. **Critical Reflections: A Student Journal on Contemporary Sociological Issues**, 2018. Disponível em: Disponível em: <https://ojs.leedsbeckett.ac.uk/index.php/SOC/article/view/4547>. Acesso em: 6 nov. 2022.

LOVELUCK, Benjamin. **Redes, liberdade e controle: uma genealogia política da internet**. 1. ed. São Paulo: Editora Vozes, 2018.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito de Viçosa**, Viçosa, v. 13, n. 1, p. 180-204, 2020.

MACHADO, Débora. A modulação de comportamento nas plataformas de mídias sociais. In: **Sociedade de Controle: Manipulação e modulação nas redes digitais**. 1. ed. São Paulo, SP. Hedra, 2018a.

MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na Sociedade Informacional: profiling e risco de discriminação**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, 2018b.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019.

MAIA, Fernanda Simplicio. Introdução ao Legítimo Interesse. In: DE LUCCA, Newton et al. **Direito & Internet IV: Sistema de proteção de dados pessoais**. São Paulo: Quartier Latin, 2019.

MALDOFF, Gabriel. **The Risk-Based Approach in the GDPR: Interpretation and Implications**. IAPP, [S.l.], 2019. Disponível em: https://iapp.org/media/pdf/resource_center/The_Risk-Based_Approach_in_the_GDPR_Interpretation_and_Implications.pdf. Acesso em: 27 nov. 2022.

MALDONADO, Viviane Nóbrega; OPICE, Renato Opice. **Lei Geral de Proteção de Dados Pessoais Comentada**. 3. ed. Revista dos Tribunais. São Paulo: 2021.

MARX, Karl. **O capital: crítica da economia política**. Livro primeiro. São Paulo: Abril Cultural, 1984.

MASUDA, Yoneji. **A Sociedade Informacional como sociedade pós-industrial**. Tradução Kival Chaves Weber e Angela Melim. Rio de Janeiro: Ed. Rio, 1982.

MAZZUCATO, Mariana. **O estado empreendedor: desmascarando o mito do setor público x setor privado**. São Paulo: Portfolio-Penguin, 2014.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. 1. ed. São Paulo: Saraiva, 2013.

MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política**. Tradução Cláudio Marcondes. São Paulo: UBU Editora, 2018.

MORRISON, Wayne. **Filosofia do Direito**: dos gregos ao pós-modernismo. São Paulo: Martins Fontes, 2006.

NEGROPONTE, N. **A Vida Digital**. São Paulo: Companhia das Letras, 1995.
OLIVEIRA, Carla. Aprendizado de máquina e modulação do comportamento humano. In: **Sociedade de Controle**: Manipulação e modulação nas redes digitais. 1. ed. São Paulo: Hedra, 2018.

OPENAI. **GPT-4 Technical Report**. 2023. Disponível em: <https://doi.org/10.48550/arXiv.2303.08774>.

ORACLE. **O que é Big Data?** Disponível em: <https://www.oracle.com/br/big-data/what-is-big-data/> . Acesso em: 6 nov. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 22 jul. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: <https://www.oecd.org/digital/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#recommendation>. Acesso em: 6 nov. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO. **OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Disponível em: <https://bit.ly/3Js9caC>. Acesso em: 6 dez. 2021.
ORWELL, George. **1984**. Tradução Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

PAMPLONA, Danielle Anne; FREITAS, Cinthia Obladen de Almendra. Exercício democrático: a tecnologia e o surgimento de um novo sujeito. **Pensar - Revista de Ciências Jurídicas**, Fortaleza, v. 20, n. 1, p. 84-107, jan./abr. 2015.

PARCHEN, Charles Emmanuel; FREITAS, Cinthia Obladen de Almendra. Crise da informação: a quem pertence? **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 2, n. 1, p. 22-38, Jan/Jun. 2016

PARDO, José Esteve. **Técnica, riesgo y derecho**. Barcelona: Ariel, 1999.

PARISER, Eli. **O Filtro invisível**: o que a internet está escondendo de você. Tradução Diego Alfaro. Rio de Janeiro: Zahar, 2012.

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

PETRAGLIA, I. C.; PALMISANO, A.; ROSINI, A. M. Alan Turing: cientista complexo e transdisciplinar. **Debates em Educação**, [S. l.], v. 12, n. 28, p.

596–609, 2020. Disponível em:
<https://www.seer.ufal.br/index.php/debateseducacao/article/view/9769>. Acesso em: 2 out. 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraivajur, 2018.

PINTO, Celciane Malcher. A sociedade de risco na visão de Ulrich Beck e suas conexões com o direito e meio ambiente. **Revista de Direito e Sustentabilidade**. Encontro Virtual, v. 7, n. 1, p. 73-91, Jan/Jul. 2021. e-ISSN: 2525-9687.

PRIOR, H., Mentira e política na era da pós-verdade: fake news, desinformação e factos alternativos. In: LOPES, P.; REIS, B. (eds.) **Comunicação Digital**: media, práticas e consumos Lisboa: NIP-@M & UAL, pp. 75-97, 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Org. Maria Celina Bodin de Moraes. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? **International Data Privacy Law**, v. 3, n. 2, p. 74-87, 2013.

RUDGARD, Sian; et al. **European Data Protection**: Law and Practice. Portsmouth: Jeanne R. Busemeyer, Hide Park Publishing Services. p. 21-52, 2018.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 26 ed. São Paulo: Malheiros, 2005.

SILVEIRA, Sérgio Amadeu. A noção de modulação e os sistemas algorítmicos. In: **Sociedade de Controle**: Manipulação e modulação nas redes digitais. 1. ed. São Paulo: Hedra, 2018.

SPALER, Mayara Guibor; REIS, Rafael Almeida Oliveira. Limites do direito fundamental à privacidade frente a uma sociedade conectada. **Revista Jurídica da Escola Superior de Advocacia da OAB/PR**, Curitiba, v. 19, n. 31, p. 47-65, 2018.

TAYLOR, Petroc. Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025. In: **Technology & Telecommunications**, 2022. Disponível em:

<https://www.statista.com/statistics/871513/worldwide-data-created/>. Acesso em: 02 fev. 2023.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. In: BIONI, Bruno (Org.) **Tratado de Proteção de Dados Pessoais**. São Paulo: Forense, 2021.

The 100 largest companies in the world by market capitalization in 2022. Economy & Politics, Economy. In: **Statista Research Department**, 2022. Disponível em: <https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/>. Acesso em: 02 fev. 2023.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data**. 2017. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 02 fev. 2023.

TURING, Alan M. Computing machinery and intelligence. **Mind**, v. 59, p. 433-460, 1950.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia (2000/C364/01)**. Jornal Oficial das Comunidades Europeias, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 18 jul. 2021.

UNITED NATIONS. **Universal Declaration of Human Rights**. Disponível em: <https://www.un.org/en/about-us/universal-declaration-of-human-rights>. Acesso em: 02 fev. 2023.

VAILSHERY, Lionel Sujay. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. In: **Technology & Telecommunications**, 2022. Disponível em: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>. Acesso em: 02 fev. 2023.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

WACHOWICZ, Marcos. O “novo” direito autoral na Sociedade Informacional. In: LEITE, José Rubens Morato; WOLKMER, Antonio Carlos. (Org.). **Os "novos" Direitos no Brasil**. 3. ed. São José dos Campos: Saraiva Jur, 2016.

WACHOWICZ, M. Os impactos das novas tecnologias da informação. **Revista do Direito**, n. 28, p. 54-89, 25 jul. 2007.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, p. 193-220, dez. 1890.

WERTHEIN, J. A Sociedade Informacional e seus desafios. **Ciência da Informação**, [S. l.], v. 29, n. 2, 2000, p. 74. Disponível em: <https://revista.ibict.br/ciinf/article/view/889>. Acesso em: 21 out. 2022.

WIMMER, Miriam. Os desafios do enforcement na LGPD: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

W3C. ABOUT W3C. Disponível em: <https://www.w3.org/Consortium/>. Acesso em 07 out. 2022.

OLIVEIRA, Carla. Aprendizado de máquina e modulação do comportamento humano. In: **Sociedade de Controle**: Manipulação e modulação nas redes digitais. 1. ed. São Paulo: Hedra, 2018.

OLIVERA, Dânton Hilário Zanetti de. **Big Data e os limites à livre iniciativa no âmbito da Lei geral de proteção de dados pessoais**. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Paraná, PPGD, 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. 1. ed. Rio de Janeiro: Intrínseca, 2020.