

**UNIVERSIDADE DE SANTA CRUZ DO SUL - UNISC**  
**PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – MESTRADO E DOUTORADO**  
**ÁREA DE CONCENTRAÇÃO EM DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS**  
**LINHA DE PESQUISA CONSTITUCIONALISMO CONTEMPORÂNEO**

Pedro Henrique Hermes

**PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE RISCO: LIMITES E**  
**POSSIBILIDADES À LIBERDADE NO AMBIENTE DIGITAL**

Santa Cruz do Sul

2023

## CIP - Catalogação na Publicação

Hermes, Pedro Henrique

PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE RISCO; : LIMITES E  
POSSIBILIDADES À LIBERDADE NO AMBIENTE DIGITAL / Pedro Henrique  
Hermes. – 2023.

137 f. ; 0 cm.

Dissertação (Mestrado em Direito) – Universidade de Santa Cruz  
do Sul, 2023.

Orientação: Prof. Dr. Rogério Gesta Leal.

1. Direitos Fundamentais. 2. Proteção de Dados Pessoais. 3.  
Liberdade Digital. 4. Sociedade de Risco. I. Leal, Rogério Gesta.  
II. Título.

Pedro Henrique Hermes

**PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE RISCO: LIMITES E  
POSSIBILIDADES À LIBERDADE NO AMBIENTE DIGITAL**

Dissertação apresentada ao Programa de Pós-Graduação em Direito – Mestrado e Doutorado – da Universidade de Santa Cruz do Sul – UNISC, linha de pesquisa Constitucionalismo Contemporâneo, como requisito parcial para obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Rogério Gesta Leal

Santa Cruz do Sul

2023

Pedro Henrique Hermes

**PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE RISCO: LIMITES E  
POSSIBILIDADES À LIBERDADE NO AMBIENTE DIGITAL**

Dissertação apresentada ao Programa de Pós-Graduação em Direito – Mestrado e Doutorado – da Universidade de Santa Cruz do Sul – UNISC, linha de pesquisa Constitucionalismo Contemporâneo, como requisito parcial para obtenção do título de Mestre em Direito.

Orientador: Prof. Dr. Rogério Gesta Leal

---

*Dr. Rogério Gesta Leal*  
Professor orientador – UNISC

---

*Dr. Janriê Rodrigues Reck*  
Professor examinador – UNISC

---

*Dr.<sup>a</sup> Alessandra Aparecida Souza Silveira*  
Professora examinadora – UMINHO

Santa Cruz do Sul

2023

## **AGRADECIMENTOS**

Ao estimado professor Dr. Rogério Gesta Leal, a quem devo meus sinceros agradecimentos pela orientação do presente trabalho, guiando e auxiliando o conhecimento aqui detalhado.

À CAPES, UNISC e ao PPGD pelo incentivo e auxílio necessário para o percurso acadêmico, bem como aos colegas do mestrado, por todo o coleguismo e debates em sala de aula.

Aos meus familiares, em especial aos meus pais Leomar e Roseli e meu irmão Samuel, que de há muito apoiam e incentivam, incondicionalmente, por minha trajetória.

A minha família do coração, Carla, Bruna, Vinícius, Gabriel e Vitória, pelo carinho e incentivo e por sempre serem tão especiais na minha vida.

Aos colegas, amigos e professores da Antonio Meneghetti Faculdade, cuja formação e ensinamentos serei eternamente grato, em especial aos professores Ricardo Schaefer e Lúcio Lorenzon.

Aos demais amigos, familiares e todos aqueles que, de uma forma ou de outra, presto meus agradecimentos por esta jornada acadêmica.

Ao meu querido Heitor, afilhado que a vida me deu, por sempre me presentear com um sorriso inocente e o carinhoso conforto do abraço de uma criança.

Por fim, à amada Débora, a quem agradeço pelo incondicional carinho, amor e compreensão desde sempre e pelo privilégio de, ao teu lado, andar pela doce estrada da vida.

## **LISTA DE SIGLAS E ABREVIATURAS**

ADC – Ação Declaratória de Constitucionalidade

ADI – Ação Direta De Inconstitucionalidade

ART – Artigo

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição da República Federativa

EC – Emenda Constitucional

GDPR - General Data Protection Regulation

LGPD – Lei Geral de Proteção de Dados

LGPD-Penal – Lei Geral de Proteção de Dados-Penal

MCI – Marco Civil da Internet

ONU – Organização das Nações Unidas

PEC – Proposta de Emenda à Constituição

STF – Supremo Tribunal Federal

## RESUMO

O presente trabalho tem por tema a liberdade e proteção de dados pessoais na Era da Informação, relacionando os direitos fundamentais na Era da informação e a Lei Geral de Proteção de Dados Pessoais – LGPD brasileira, promulgada em 2018, diante da Sociedade de Risco. O problema de pesquisa da dissertação é a seguinte: como o direito fundamental à liberdade no ambiente digital pode ser amparado pelo direito fundamental à proteção de dados pessoais e a Lei nº. 13.708/18 (Lei Geral de Proteção de Dados Pessoais), a partir do âmbito de proteção, tutelando o direito fundamental na Era da Informação, especialmente diante da Sociedade de Risco? A hipótese inicial deste trabalho é a de que a proteção de dados pessoais representa, nomeadamente no Brasil, importante avanço em face das relações que ocorrem no ambiente digital, em especial tendo presente a Sociedade de Riscos, principalmente a partir dos princípios norteadores do tratamento de dados previstos na LGPD, do papel que o consentimento assume enquanto base legal para o tratamento de dados e expressão da liberdade, bem como pela criação de uma Autoridade Nacional de Proteção de Dados Pessoais, na atuação fiscalizatória, judicante e legiferante no Brasil. O objetivo geral é verificar em que medida a Lei Geral de Proteção de Dados brasileira pode contribuir à tutela de direitos fundamentais relacionados ao que ela disciplina na Sociedade de Riscos e na Era da Informação em que nos encontramos, muito especialmente em ambientes virtuais. Os objetivos específicos são: estudar o fenômeno da Era da Informação e suas consequências, a partir das bases teóricas da Sociedade em Rede e Sociedade de Risco; analisar os elementos dos direitos fundamentais à privacidade e liberdade como direitos que tutelam a pessoa em ambientes virtuais diante da Sociedade de Risco; verificar os desdobramentos do direito fundamental de proteção de dados pessoais e da LGPD brasileira no ambiente digital e as possibilidades que tais elementos permitem à tutela do direito de liberdade no ambiente digital. A proposta da pesquisa se vincula à linha de pesquisa Constitucionalismo Contemporâneo do Programa de Pós-Graduação em Direito da Universidade de Santa Cruz do Sul na medida em que aborda a sociedade da informação em sua complexidade e suas consequências nos direitos e garantias fundamentais da pessoa a partir do fenômeno constitucional, notadamente acerca do surgimento de novos direitos fundamentais decorrentes do desenvolvimento digital, especialmente na Era da Informação. A temática se encontra adequada às pesquisas do professor orientador, tendo em vista que aborda os direitos fundamentais e a proteção de dados pessoais a partir da compreensão do conceito de Sociedade de Risco. Para responder à problemática, utilizar-se-á como método de abordagem o dedutivo, porquanto aborda as mudanças sociais a partir das novas tecnologias, perpassando sobre proteção dos direitos fundamentais, a fim de verificar, como a proteção de dados pessoais pode tutelar os direitos de liberdade. Como método de procedimento utilizar-se-á o monográfico, porquanto a pesquisa será realizada com base em revisão de bibliografia. A pesquisa se utilizará, ainda, da técnica da documentação indireta, com consulta em bibliografia de fontes secundárias como jornais, artigos científicos, revistas especializadas na área da pesquisa, livros e demais textos acadêmicos.

**Palavras-chave:** ambiente digital; direitos fundamentais; liberdade; proteção de dados pessoais; Sociedade de Risco.

## ABSTRACT

The present work has as its theme the freedom and protection of personal data in the Information Age, relating fundamental rights in the Information Age and the Brazilian General Law for the Protection of Personal Data - LGPD, enacted in 2018, before the Sociedade de Risco. The research problem of the dissertation is the following: how the fundamental right to freedom in the digital environment can be supported by the fundamental right to the protection of personal data and Law n<sup>o</sup>. 13.708/18 (General Law for the Protection of Personal Data), from the scope of protection, protecting the fundamental right in the Information Age, especially in the face of the Risk Society? The initial hypothesis of this work is that the protection of personal data represents, particularly in Brazil, an important advance in the face of the relationships that occur in the digital environment, especially bearing in mind the Risk Society, mainly from the guiding principles of data processing. data provided for in the LGPD, the role that consent assumes as a legal basis for the processing of data and the expression of freedom, as well as the creation of a National Authority for the Protection of Personal Data, in the supervisory, judging and legislating role in Brazil. The general objective is to verify to what extent the Brazilian General Data Protection Law can contribute to the protection of fundamental rights related to what it disciplines in the Risk Society and in the Information Age in which we find ourselves, especially in virtual environments. The specific objectives are: to study the phenomenon of the Information Age and its consequences, based on the theoretical bases of the Network Society and Risk Society; analyze the elements of the fundamental rights to privacy and freedom as rights that protect the person in virtual environments in the face of the Risk Society; verify the developments of the fundamental right to protection of personal data and the Brazilian LGPD in the digital environment and the possibilities that such elements allow for the protection of the right to freedom in the digital environment. The research proposal is linked to the Contemporary Constitutionalism research line of the Graduate Program in Law at the University of Santa Cruz do Sul insofar as it addresses the information society in its complexity and its consequences on the fundamental rights and guarantees of the person to from the constitutional phenomenon, notably about the emergence of new fundamental rights resulting from digital development, especially in the Information Age. The theme is suitable for research by the advisor professor, considering that it addresses fundamental rights and the protection of personal data based on the understanding of the concept of Risk Society. To answer the problem, the deductive approach will be used as a method of approach, as it addresses social changes from new technologies, passing through the protection of fundamental rights, in order to verify how the protection of personal data can protect the rights of freedom. As a method of procedure, the monographic will be used, since the research will be carried out based on a bibliography review. The research will also use the technique of indirect documentation, with consultation in the bibliography of secondary sources such as newspapers, scientific articles, magazines specialized in the area of research, books and other academic texts.

**Keywords:** digital environment; fundamental rights; freedom; protection of personal data; Risk Society.

## SUMÁRIO

<b>INTRODUÇÃO.....</b>	<b>9</b>
<b>1 A SOCIEDADE EM REDE COMO SOCIEDADE DE RISCOS - ASPECTOS PERFORMATIVOS.....</b>	<b>14</b>
1.1 A Era da Informação e a Sociedade em Rede: do nascimento das redes aos dados pessoais no ambiente digital .....	15
1.2 A Sociedade de Risco: entre as incertezas da modernidade reflexiva e os riscos globais .....	25
1.3 A Rede como Risco: a Era da Informação e os riscos da Internet.....	33
<b>2. DIREITOS FUNDAMENTAIS E INTERNET: LIBERDADE E PRIVACIDADE FRENTE AOS RISCOS DA REDE .....</b>	<b>47</b>
2.1 Breve excursão sobre a teoria dos direitos fundamentais na Constituição de 1988 e a Era da Informação.....	47
2.2 O direito fundamental à liberdade e seus novos contornos na Sociedade de Risco.....	58
2.3 Privacidade, vigilância e riscos: âmbito de proteção e (in)suficiência frente a automatização das informações na Internet.....	69
<b>3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: POSSIBILIDADES À LIBERDADE NA ERA DA INFORMAÇÃO.....</b>	<b>82</b>
3.1 Fundamentos para o direito fundamental à proteção de dados pessoais ....	83
3.2 Considerações sobre o sistema jurídico brasileiro de proteção de dados pessoais.....	94
3.3 A proteção jurídica dos dados pessoais e a proteção e limites à liberdade no ambiente digital: caminhos para possibilidade da liberdade na Era da Informação e da Sociedade de Risco.....	107
<b>CONCLUSÃO.....</b>	<b>121</b>
<b>REFERÊNCIAS .....</b>	<b>127</b>

## INTRODUÇÃO

O “mundo on-line” cada vez mais se faz presente na “realidade off-line”. Seja nas relações de amizade, comerciais, compartilhamento de informações, fotos e vídeos, entre tantas outras possibilidades que a Internet oferece, a relação de distanciamento entre esses dois “mundos” se mostra mitigada a ponto da tecnologia integrar o ser humano e seu cotidiano. Redes sociais, *e-commerce*, smartphones, microchips, relógios inteligentes, aparelhos domésticos inteligentes, rastreamento de localização, entre outros, se tornam mecanismos comuns em razão do fenômeno de redução (ou fim) das distâncias entre esses mundos.

O digital faz parte do real e o real integra o digital. Mesmo não desejando, não acessando ou utilizando qualquer mecanismo, é inevitável que alguma de nossas informações se encontre nesse ambiente, muito devido à informatização e constituição de redes de informação no ambiente digital.

Na base de todos esses contextos, encontram-se dois pontos primordiais para se analisar o fenômeno: as informações e dados pessoais que são inseridos no ambiente digital e as consequências à liberdade, seja no meio digital, seja na realidade.

Desses impactos, extrai-se que a pessoa/usuária se encontra sempre suscetível à infinidade dos riscos decorrentes do uso dessas tecnologias, sobretudo os riscos à personalidade e à liberdade, em razão de que operações com dados pessoais são essenciais nesses cenários e para o desenvolvimento das tecnologias e do avanço científico e mercadológico. Na atualidade, impossível se falar na não utilização desses instrumentos. Em verdade, necessário se debater formas e mecanismos de se reduzir quaisquer riscos associados.

Denota-se que a evolução das legislações, sobretudo as constitucionais, busca acompanhar o movimento de tutela das pessoas nas Cartas de cada país, de modo a reduzir, de alguma forma, riscos inerentes às atividades no ambiente digital. De outro lado, percebe-se que a evolução humana, na atualidade, impescinde da evolução tecnológica, nomeadamente o desenvolvimento das pesquisas científicas de base tecnológica, estratégias de mercado pela centralidade da economia digital.

Constata-se que são inúmeras forças a serem equacionadas nessas difíceis relações, cujas tensionalidades são também inúmeras. O papel dos direitos fundamentais é central e crucial como marco interpretativo dessas equações,

ocupando eles a verdadeira função de, por um lado, tutelar a pessoa humana no ambiente digital e para além dele, e, de outro, assegurar que todas as relações que impactem com esse ambiente sejam pautadas na proteção dos direitos fundamentais.

Logo, os direitos de liberdade e proteção de dados pessoais são elementos necessários para se pautar essas tensionalidades, principalmente diante das consequências da Sociedade de Risco, ou seja, a sociedade cujo risco, invisível e imperceptível, se faz cada vez mais presente nas relações sociais.

Nesse sentido, o presente trabalho tem por tema a liberdade e proteção de dados pessoais na Era da Informação, relacionando os direitos fundamentais na Era da informação e a Lei Geral de Proteção de Dados Pessoais – LGPD brasileira, promulgada em 2018, diante da Sociedade de Risco.

Diante disso, a problemática central da presente dissertação é a seguinte: como o direito fundamental à liberdade no ambiente digital pode ser amparado pelo direito fundamental à proteção de dados pessoais e a Lei nº. 13.708/18 (Lei Geral de Proteção de Dados Pessoais), a partir do âmbito de proteção, tutelando o direito fundamental na Era da Informação, especialmente diante da Sociedade de Risco?

A hipótese inicial deste trabalho é a de que a proteção de dados pessoais representa, nomeadamente no Brasil, importante avanço em face das relações que ocorrem no ambiente digital, em especial tendo presente a Sociedade de Riscos em que vivemos, principalmente a partir dos princípios norteadores do tratamento de dados previstos na LGPD, do papel que o consentimento assume enquanto base legal para o tratamento de dados e expressão da liberdade, bem como pela criação de uma Autoridade Nacional de Proteção de Dados Pessoais, na atuação fiscalizatória, judicante e legiferante em relação à temática no Brasil.

Por conseguinte, tem-se como o objetivo geral verificar em que medida a Lei Geral de Proteção de Dados brasileira pode contribuir à tutela de direitos fundamentais, nomeadamente a liberdade, relacionados ao que ela disciplina na Sociedade de Riscos e na Era da Informação em que nos encontramos, muito especialmente em ambientes digitais.

De outro lado, os objetivos específicos são os seguintes: estudar o fenômeno da Era da Informação e suas consequências, a partir das bases teóricas da Sociedade em Rede e Sociedade de Risco; analisar os elementos dos direitos fundamentais à privacidade e liberdade como direitos que tutelam a pessoa em

ambientes virtuais diante da Sociedade de Risco; verificar os desdobramentos do direito fundamental de proteção de dados pessoais e da LGPD brasileira no ambiente digital e as possibilidades que tais elementos permitem à tutela do direito de liberdade no ambiente digital.

Nesse sentido, denota-se que a temática da pesquisa se mostra atual, relevante e convergente com as necessidades advindas das novas dinâmicas normativas oriundas do contexto da Era da Informação, posto que visa analisar como se portam os direitos fundamentais nesse novo contexto, especialmente a partir do surgimento da Internet, e de como o direito à proteção de dados, visto como um direito fundamental, se faz necessário para a tutela dos indivíduos e da sua liberdade no ambiente digital proporcionado pelas novas tecnologias. Além disso, a contribuição para o meio acadêmico vem demonstrada pela possibilidade de se conferir uma adequada releitura desses direitos diante dos novos contornos trazidos pela Internet, uma vez que causam inúmeras mudanças sociais, econômicas e jurídicas.

A proposta da pesquisa em apreço também se vincula a linha de pesquisa Constitucionalismo Contemporâneo do Programa de Pós-Graduação em Direito da Universidade de Santa Cruz do Sul na medida em que visa abordar a sociedade da informação em sua complexidade e suas consequências nos direitos e garantias fundamentais da pessoa a partir do fenômeno constitucional, notadamente acerca do surgimento de novos direitos fundamentais decorrentes do desenvolvimento digital e suas repercussões sociais. Além disso, a temática se encontra adequada às pesquisas do professor orientador Rogério Gesta Leal, tendo em vista que aborda os direitos fundamentais e a proteção de dados pessoais a partir da compreensão do conceito de Sociedade de Risco, especialmente diante de seus impactos na sociedade e o agir estatal.

Para responder à problemática colocada, utilizar-se-á como método de abordagem o dedutivo, partindo da compreensão geral acerca das mudanças sociais possibilitadas pelas novas tecnologias, perpassando sobre os direitos fundamentais e sua proteção no atual contexto constitucional, a fim de verificar, especificamente, como a proteção de dados pessoais pode tutelar os direitos de liberdade. Como método de procedimento utilizar-se-á o monográfico, porquanto a pesquisa será realizada com base em revisão de bibliografia. Com isso, pretende-se aprofundar a temática a partir de uma premissa geral, qual seja a Sociedade de Risco e os

direitos fundamentais, até a premissa menor, que é tratar da relação liberdade digital e proteção de dados, sendo tudo isso amparado em pesquisas precedentes.

A pesquisa se utilizará, ainda, da técnica da documentação indireta, com consulta em bibliografia de fontes secundárias como jornais, artigos científicos, revistas especializadas na área da pesquisa, livros e demais textos acadêmicos dentro da temática proposta.

O primeiro capítulo se dedicará à abordagem de suas teorias essenciais para compreensão da evolução tecnológica e os impactos decorrentes: a Sociedade em Rede e a Sociedade de Risco. São consideradas, para fins do presente trabalho, como possíveis de interpretação conjunta, apesar de suas particularidades e aspectos, como o temporal e o espectro de análise.

A Sociedade em Rede marca, sobretudo, o aspecto da propulsão do surgimento das redes em decorrência do fenômeno tecnológico, explicitando os impactos sociais e econômicos decorrentes. Nesse sentido, para a sua compreensão e detalhamento teórico, optou-se por utilizar os escritos de Manuel Castells, principal expoente da teoria. Por sua vez, a Sociedade de Risco aborda os problemas da modernidade em relação ao aumento de riscos, nomeadamente no pós-Revolução Industrial, e também sobre a metamorfose digital, fenômeno que impacta diretamente na produção de riscos no ambiente digital.

Importante destacar, de início, a preferência teórica da presente pesquisa pelos autores centrais das suas teorias: Manuel Castells, acerca da Sociedade em Rede, e Ulrich Beck, sobre a Sociedade de Risco. Isso pelo fato dos dois autores tratarem, no conjunto de suas obras, essencialmente dos impactos que a tecnologia da informação exerce sobre as realidades. Essa preferência teórica se mostra, por sua vez, justificada pelo fato de se tratarem de teóricos expoentes de cada. Essa preferência não significa não se utilizar de referências a outros autores sobre as temáticas trazidas, pelo contrário, na medida em que contribuirão para a compreensão do contexto.

Por sua vez, o segundo capítulo abordará sobre três pontos essenciais que subsidiarão possíveis respostas ao problema de pesquisa: a teoria dos direitos fundamentais, o direito de liberdade e o direito à privacidade. Aliando-se à perspectiva tradicional sobre esses direitos, tais pontos serão analisados à luz dos impactos que o ambiente digital traz especialmente aos direitos fundamentais, separadamente. Tratando-se de pesquisa versando sobre direitos fundamentais,

inevitável lançar mão de escritos e autores clássicos sobre cada uma das temáticas, sem olvidar da conexão com autores que conjugam a leitura clássica com o impacto das tecnologias, como, por exemplo, Ingo Wolfgang Sarlet, preferência que se justifica pela contribuição teórica aos direitos fundamentais, sobretudo nas suas relações com o ambiente digital.

O terceiro capítulo se debruçará sobre a questão essencial do presente trabalho: a relação entre dados pessoais e a liberdade no ambiente digital enquanto direitos fundamentais. Em se tratando de direitos fundamentais no ambiente digital, denota-se que a complexidade para análise é inerente ao fenômeno, de modo que não há pretensão de exaustão da temática por esta pesquisa, mas de, a partir do problema de pesquisa proposto, oferecer elementos ao debate sobre as relações entre Sociedade de Risco, direitos fundamentais, dados pessoais e liberdade no ambiente digital.

Importante destacar que, apesar de se tratar de uma pesquisa essencialmente sobre direitos fundamentais, mas em cujo problema de pesquisa também se encontra a baliza de uma lei infraconstitucional (LGPD), em grande medida o debate se mostrará dialogado entre esses dois aspectos, objetivando fazer uma análise sobre a temática. Além disso, menciona-se que a pretensão é de mostrar como esse sistema jurídico de proteção de dados pessoais poderá tutelar a liberdade no espaço digital.

## **1 A SOCIEDADE EM REDE COMO SOCIEDADE DE RISCOS - ASPECTOS PERFORMATIVOS**

O presente capítulo abordará as teorias sociológicas da Sociedade em Rede e da Sociedade de Risco, buscando compreender, essencialmente, o fenômeno do desenvolvimento tecnológico iniciado pelo surgimento da Internet e da informática, pautado na formação e criação de redes e estruturas de redes responsáveis por diversas transformações econômicas, sociais, culturais e também jurídicas, e de como esses fenômenos podem ser geradores de riscos em nossa sociedade, notadamente aos direitos fundamentais, com especial enfoque na privacidade, dados pessoais e liberdade.

Para visualizar e entender a Era da Informação será abordado primeiramente o marco teórico da Sociedade em Rede, a partir da proposta teórica do sociólogo Manuel Castells em seus escritos. Essa construção iniciará a partir da descrição daquilo que foi e é o desenvolvimento das redes, sobretudo através da Internet, buscando descrever a sociedade informacional e de como ela, ao longo do tempo, se constituiu e constitui uma Sociedade em Rede pautada na informação e na ampliação da comunicação, além da globalização como fator determinante para formação dessas “novas” redes.

Posteriormente, será realizado um percurso teórico sobre a teoria da Sociedade de Riscos, proposta basicamente por Ulrich Beck, abordando conceitos essenciais em sua teoria, tais como risco, efeito bumerangue, globalização, metamorfose digital, entre outros. Por sua vez, então no terceiro momento, serão buscados subsídios para visualizar como a Sociedade em Rede evidencia determinados riscos, especialmente diante da utilização das informações e dos dados pessoais<sup>1</sup> como mecanismo central de funcionamento e economia, o que será abordado ainda de modo mais profundo no decorrer da pesquisa.

Destaca-se que, como já feito na introdução, que há a preferência na utilização dos dois autores como marco teórico, não se olvidando outros escritos sobre as

---

<sup>1</sup> O conceito de dados pessoais permeará quase que a totalidade do presente trabalho, mas não será integralmente abordado no presente capítulo. Todavia, uma conceituação mínima já nesse momento se faz necessária para uma adequada compreensão do que se está a transmitir. Nesse momento, adota-se o conceito legal de dados pessoais, previsto no artigo 5º, inciso I da Lei Geral de Proteção de Dados Pessoais, qual seja a “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018).

temáticas por outros reconhecidos autores com profundidade teórica. No entanto, ressalta-se que ambos, no conjunto de sua obra, analisam o fenômeno da Internet e do ambiente digital, cujas contribuições interessam para a presente pesquisa.

Adentrar nessas teorias é relevante para se compreender a organização e estruturação social na qual se encontra o Direito, especialmente os direitos fundamentais e as suas transformações na sociedade informacional, gerando modificações, por exemplo, no direito fundamental à privacidade, liberdade, entre outros. Nesse sentido, os acontecimentos e transformações sociais, visualizados a partir das teorias sociológicas em apreço, fornecerão sustentáculo teórico para ampla discussão dos direitos fundamentais nesses espaços, notadamente de como o Direito deve operar no ambiente da Sociedade de Risco.

### **1.1 A Era da Informação e a Sociedade em Rede: do nascimento das redes aos dados pessoais no ambiente digital**

O percurso histórico da humanidade é marcado pela progressão e desenvolvimento tecnológico como forma de se alcançar maior qualidade nas ações humanas. Apesar de não ser o objetivo do presente estudo, é sabido que as noções de progresso e desenvolvimento são teoricamente controvertidas, especialmente os impactos que as tecnologias exercem nessa compreensão. Contudo, não se deve negar que o que se denomina como desenvolvimento tecnológico acarreta transformações sociais, econômicas, jurídicas e as consequências trazida pela Internet podem ser consideradas como tais fenômenos.

Com o advento da Internet e as transformações sociais dela decorrentes, ascenderam novas formas de comunicação e ferramentas, além do surgimento de uma nova economia, cultura e também de sociedade, pautada na informação e no desenvolvimento tecnológico. A essa nova forma de estruturação social, centrada na tecnologia da informação, deu-se o nome de Era da Informação<sup>2</sup>. O seu surgimento é comparado por alguns às Revoluções Industriais que também transformaram contextos, economias e a sociedade. Entretanto, para outros teóricos a revolução da

---

<sup>2</sup> Há aqui uma questão teórica a ser apontada, pois o que se quer significar com o termo Era da Informação também pode ser encontrado como sociedade informacional ou sociedade da informação. O marco teórico aqui adotado não traz relevante divergência sobre tal aspecto. Contudo, desde já, e como se verá ao longo do texto, destaca-se que tais termos não são sinônimos de Sociedade em Rede, pois a sociedade informacional vai além do conceito proposto por Castells de Sociedade em Rede.

Era da Informação é diferente da proporcionada pelas Revoluções Industriais, seja em sua formação, seja em suas consequências, dado o acelerado passo dessas transformações na sociedade.

A partir da proposta teórica de Manuel Castells, essa Era da Informação pode ser visualizada sob a perspectiva de constituição de redes, fortalecendo, segundo o autor, a Sociedade em Rede (CASTELLS, 2016, p. 61). No entanto, antes de se analisar mais detidamente tal conceito, necessário se fazer uma breve incursão sobre o surgimento da Internet, especialmente diante da relevância que essa compreensão possui para a presente pesquisa, haja vista que se está a estudar os direitos fundamentais no ambiente informacional.

Se analisado o percurso da história e o desenvolvimento tecnológico correspondente, observa-se que o fenômeno da Internet é relativamente recente, mas que se encontra em ritmo acelerado. Não obstante as já conhecidas inovações sociais e tecnológicas desde o surgimento da informática, além dos avanços da humanidade a partir do uso das novas tecnologias desde então, o que despontou como principal finalidade da Internet em sua gênese foi o aspecto militar.

Souza (2014, p. 54-55) lembra que os primeiros passos para o que posteriormente se chamou de Internet iniciaram no ano de 1962, época em que o Departamento de Defesa dos Estados Unidos lançou o projeto ARPA, com o objetivo de evitar o colapso em seu sistema de comunicação pelos soviéticos, período da Guerra Fria, descentralizou, então, o seu centro de comunicações.

Além disso, considerando que o Departamento possuía colaborações com universidades e centros de pesquisas do país para o aprimoramento científico, essa rede instaurada também foi amplamente utilizada por tais agentes no âmbito da pesquisa científica e relação universitária. Entretanto, além da utilização para as pesquisas militares pelo Departamento de Defesa, os cientistas usaram a rede para suas próprias comunicações, instaurando uma rede própria para troca de mensagens entre cada um dos cientistas e universidades, ampliando as finalidades e centros de operação (CASTELLS, 2016, p. 101).

Ao longo das décadas seguintes, desenvolveram-se outras redes além da ARPANET, havendo uma cisão da rede utilizada para fins militares e a rede para utilizada para fins de pesquisa, em razão de que as finalidades passaram a se confundir com o uso cotidiano para troca de informações e comunicação entre pesquisadores e órgãos militares. Pouco a pouco, formaram-se redes de redes,

estruturas que passaram a conectar diversos centros científicos e universidades, permitindo a ampla difusão da Internet e a maior descentralização das informações, até a substituição da ARPANET pela rede NSFNET, ocasionando ao final a retirada da rede ARPANET (CASTELLS, 2003, p. 15), em um movimento que iniciou a desestatização da rede, pois se tratava, em sua essência, de um projeto estatal-militar.

O ápice da liberalização estatal e popularização daquilo que hoje é a Internet ocorreu em meados dos anos de 1990, quando a tecnologia das redes de computadores passou para o domínio público alicerçando a interconexão de redes e a operação privada da Internet quando a National Science Foundation, nos Estados Unidos, deixou de ter o seu controle (CASTELLS, 2003, p. 15).

Outro grande salto para a maciça utilização e proliferação da rede ocorreu com a criação do sistema *world wide web*, conhecido pelas suas três letras iniciais *WWW*<sup>3</sup>, permitindo a organização de todos os endereços constantes na internet em razão das informações que possuem, não pela localização, facilitando sobremaneira o acesso aos conteúdos pelos usuários conectados à rede (CASTELLS, 2016, p. 105). A criação desse sistema permitiu maior abertura da rede, ampliando a quantidade de usuários.

Tendo seu início nos anos de 1960 e sua popularização a partir de 1990, pelos motivos brevemente descritos, Castells (2003, p 13) aduz que o desenvolvimento da Internet “põe em relevo a capacidade que têm as pessoas de transcender metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo”.

A afirmação decorre do fato que o princípio de utilização da rede sequer foi o propulsor de sua difusão, tendo em vista que a finalidade militar e estatal não foi atingida nos projetos iniciais para o desenvolvimento da Internet, sendo muito importante, na verdade, a atuação dos centros de pesquisa e universidades para que fosse conhecida da maneira que é hoje, pois, a partir das trocas de informações e do interesse dos cientistas, foi possibilitado um amplo desenvolvimento desse sistema de comunicação.

---

<sup>3</sup> O surgimento da *WWW*, ainda na década de 1990, aproximadamente 30 anos do projeto Arpanet, demonstra a rápida difusão da rede ao longo do mundo, haja vista que a invenção da *WWW* ocorreu em um dos principais centros de pesquisa em física do mundo, o CERN, em Genebra, que o distribuiu gratuitamente (CASTELLS, 2016, p. 106). Essa ampla e rápida difusão da Internet, e também de seu contínuo aperfeiçoamento, demonstra a agilidade dos processos ocorridos desde o início da Era da Informação.

Como bem pontua Castells (2016, p. 100), o surgimento da Internet se deve a uma “fusão singular de estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural”. Contracultural, pois a cultura *hacker* e os ideais libertários foram também essenciais para se chegar aos resultados dos dias atuais. Pode-se acrescentar também que a sua difusão foi possível pela liberdade de mudanças e crescimento da rede, pois ela “se desenvolveu num ambiente seguro, propiciado por recursos públicos e pesquisa orientada para missão, mas que não sufocava a liberdade de pensamento e inovação” (CASTELLS, 2003, p. 24), mesmo havendo o contexto e pressão da Guerra Fria durante aquele período.

Souza (2014, p. 56) destaca que essa ampla difusão também se deve ao aperfeiçoamento dos computadores, capacidade de memória e transmissão dos dados. Além disso, a expansão na década de 1990 também ocorreu em razão da difusão da comunicação sem fio (CASTELLS, 2019, p. 36), aliado ao grande desenvolvimento tecnológico em relação a *microchips*, telefonia, telecomunicações, entre outros.

Nesse sentido, Lévy (2010, p. 31) acrescenta que a computação permitiu o incremento na produção industrial, automação do terceiro setor, que objetivou aumentar a produtividade pelo uso dos equipamentos eletrônicos e dos dados. Dessa maneira, não apenas influenciou na modificação da comunicação, mas foi propulsora, de modo não intencional, de uma nova forma das relações econômicas e sociais.

A Internet é possuidora de características próprias que a faz ser o que é. Talvez a principal delas seja a sua descentralização, haja vista que não possui um centro operacional próprio que comande e ordene as suas operações, mas justamente é marcada pela sua estruturação em redes com diferentes nós. Aliado a isso, é marcante a desterritorialização, considerando que, apesar de cada Estado regular o seu uso, não possui um território próprio, ou seja, a sede da Internet<sup>4</sup>. Apesar de esses fatores terem sido determinantes para a disseminação da Internet como ela é, observa-se que, pouco a pouco, tais características se mostram tensionadas frente às necessidades de regulação, como se verá mais adiante.

Fato é que “a Internet é um meio de comunicação que permite, pela primeira

---

<sup>4</sup> Importante aqui já se fazer o destaque à ADC 51, que versa sobre o compartilhamento de dados de comunicação privada para fins de persecução penal, situados no exterior. O tema será abordado nos capítulos seguintes, mas a temática demonstra a complexidade da questão frente à desterritorialidade da Internet.

vez, a comunicação de muitos com muitos, num momento escolhido, em escala global” (CASTELLS, 2003, p. 08), possibilitando que se reforçasse uma forma de organização da sociedade, que Castells conceitua como Sociedade em Rede. Para o autor, atualmente essa Sociedade

é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes [...] E os nós são, em linguagem formal, os pontos onde a curva se intersecta a si própria [...] (CASTELLS, 2005, p. 20).

Vale destacar que a Sociedade em Rede não surgiu exclusivamente a partir da Internet. Na verdade, a Internet e o desenvolvimento tecnológico aliado a ela intensificou o processo de formação das redes, permitindo sua expansão ao nível global. O conceito de Sociedade em Rede, logo, não se limitaria a essa nova forma social, política e econômica oriunda do fenômeno da internet, mas, na verdade, sua perspectiva foi ampliada a partir das tecnologias da informação, fortalecendo as redes (CASTELLS, 2005). Gize-se que a “formação de redes é uma prática humana muito antiga, mas as redes ganharam vida nova em nosso tempo transformando-se em redes de informação energizadas pela Internet” (CASTELLS, 2003, p. 07)<sup>5</sup>.

Em outras palavras, as redes se intensificaram a partir do desenvolvimento tecnológico e comunicacional decorrente da Internet. A sociedade informacional, portanto, é uma Sociedade em Rede, mesmo que algumas de suas características englobam funções que vão além do sistema das redes (CASTELLS, 2016, p. 85). Oliveira e Cremonini (2019, p. 5169-5170) referem que a Sociedade em Rede

[...] trata-se de uma sociedade de contornos globais e cenários transnacionais, centrada na tecnologia da informação, no uso da comunicação instantânea, sobremaneira constituída por um padrão sofisticado de complexas redes, redes de redes interligadas, versátil em seu modelo aberto e flexível, onde a informação é gerada, processada, armazenada, recuperada e transmitida instantaneamente, constituindo o seu ciclo de alimentação e realimentação cumulativo entre a contínua inovação e o seu uso.

Como Castells refere, “a comunicação em rede transcende fronteiras, a

---

<sup>5</sup> Aliás, a formação de redes de cooperação entre seres humanos, conforme lição de Harari (2020, p. 184) é um dos fatores tidos pelo autor como essenciais para a sobrevivência do *homo sapiens*, de forma que, em função da organização em redes de cooperação de massa, foi possível a estrutura e organização social do ser humano.

sociedade em rede é global, é baseada em redes globais”, sendo que ao que “chamamos globalização é outra maneira de nos referirmos à sociedade em rede, ainda que de forma mais descritiva e menos analítica do que o conceito de sociedade em rede implica” (CASTELLS, 2005, p. 18). Dessa maneira, assim como a Internet, a Sociedade em Rede também se manifesta em caráter global e está relacionado ao que se quer dizer com globalização.

Nesse sentido, referem Oliveira e Cremonini (2019, p. 5161), que “o fenômeno da rede projetou-se até os presentes dias e contemporaneamente constitui uma de suas principais e impactantes características globais” No que toca à globalização, conforme Baumann (1999, p. 07), é assunto que “está na ordem do dia”, principalmente se tomado o contexto a partir do Segundo Pós-Guerra, da Guerra Fria e do surgimento das redes através da Internet, onde a economia, a informação, entre outros, tornaram-se assunto global.

Oliveira e Cremonini (2019, p. 5165) descrevem aquilo que nominam como Revolução da Tecnologia Informacional, fenômeno que “pode ser considerado o mais importante das últimas duas décadas do século XX, evoluindo e avançando com muita solidez até os presentes dias, configurando-se por meio de uma sociedade constituída por redes de força e poder” (p. 5165). Os autores colocam essa revolução ao mesmo nível da globalização, ambos ocorridos após a Segunda Guerra. Castells ainda asseverando o caráter de globalidade das redes digitais quando afirmam que “as redes digitais são globais, pois têm a capacidade de se reconfigurar de acordo com as instruções de seus programadores, ultrapassando fronteiras territoriais e institucionais por meio de redes telecomunicadas de computadores” (CASTELLS, 2019, p. 71).

Acerca da Internet e seu caráter global, observa-se que ela transcende quaisquer fronteiras e escapa ao controle dos Estados, além de não ser uma rede regulamentada de maneira uniforme, pois diferentes países a regulam de diferentes maneiras – o que possui conexão com o regime político adotado por determinado Estado<sup>67</sup>. Nesse ponto, referem Oliveira e Cremonini que “com o uso a tecnologia da

---

<sup>6</sup> A questão também encontra amparo na ideia de Estado de Exceção e de como o Direito pode ser utilizado para essa finalidade. Leal (2020, p. 361) traz o exemplo do Estado de Urgência promovido na França a partir de ataques em Paris, no ano de 2015, sob o fundamento da segurança pública e nacional, onde restou autorizada a promoção acesso a domicílios sem autorização judicial, devassando-se a privacidade do morador em nome de tais direitos.

<sup>7</sup> Por estar ligada ao acesso à informação e ampliação do poder de comunicação dos cidadãos, obviamente a internet é regulamentada de modo diverso em países de regime democrático e países

informação tudo interconecta-se por meio de múltiplos canais e virtualmente se comunica”. Isso permite que “as ideias fluem pelas redes *intra* e *inter* computadorizadas, ligando empresas, cidades, Estados, instituições, organizações, movimentos, indivíduos, além de uma grande e emergente variedade de atores não estatais” (OLIVEIRA: CREMONINI, 2019, p. 5165).

É importante referir que Castells define a Rede como “um conjunto de nós interconectados” (CASTELLS, 2003, p. 07), declarando, em outro momento, que as Redes “são estrutura abertas capazes de expandir de forma ilimitada, integrando novos nós desde que consigam comunicar-se dentro da rede, ou seja, desde que compartilhem os mesmo códigos de comunicação” (CASTELLS, 2016, p. 554), evidenciando que redes são, de fato, estruturas elásticas que podem se expandir, desde que existam condições para que haja adequada comunicação entre os nós e também das próprias redes.

Destaca-se que a comunicação constitui um ponto fulcral no conceito de Sociedade em Rede, haja vista que é da essência humana o ato de comunicação, que se modificou com a disseminação da Internet, propiciando um novo ambiente para ela (CASTELLS, 2003, p. 225). Nesse sentido, na obra *O Poder da Comunicação*, Castells disserta sobre como a comunicação se transformou no seio da Sociedade em Rede e como essas redes também constituem um poder, sobretudo quando o poder se centralizou nas redes de comunicação.

Contudo, as transformações ocorridas a partir da Internet não apenas reforçaram as redes e a comunicação. Erigiu-se um novo e promissor mercado, iniciando uma nova era na economia capitalista baseada na informação. Castells (2016, p. 135) denomina essa economia como informacional, global e em rede, haja vista que os seus processos dependem da informação gerada e produzida para o conhecimento, da organização em escala global e da constituição de redes empresariais para seu desenvolvimento, sendo indispensavelmente erigida a partir da revolução tecnológica. Como assevera Castells

---

de regime ditatorial. Nesse sentido, ao passo que nos Estados Unidos a regulação e legislação sobre a Internet possui um caráter mais liberal – cujas origens remontam à própria história do Estado e a noção de liberdade, em países ditatoriais, como no caso da Coreia do Norte, a regulamentação é mais rígida, com maiores restrições aos cidadãos e maior controle do Estado sobre as informações. Caso semelhante é o da China, que, em relação aos dados pessoais dos usuários, busca ter maior controle, como quando ocorreu durante a pandemia de coronavírus, onde o Estado buscou amplamente monitorar os cidadãos para se evitar a transmissão do vírus, fato que não foi repetido em países conceituados como democráticos, como o Brasil.

A sociedade em rede, em suas várias expressões institucionais, por enquanto é uma sociedade capitalista. Ademais, pela primeira vez na história, o modo capitalista de produção dá forma às relações sociais em todo o planeta. Mas esse tipo de capitalismo é profundamente diferente de seus predecessores históricos. Tem duas características distintas fundamentais: é global e está estruturado, em grande medida, em uma rede de fluxos financeiros (CASTELLS, 2016, p. 555).

Do mesmo modo, alguns elementos são determinantes para essa nova economia baseada na inovação tecnológica, quais sejam a lucratividade e a competitividade, além da própria produtividade (CASTELLS, 2016, p. 151). Nesse sentido, observa-se que a produtividade e a competitividade se fundamentam na geração do conhecimento, o que está relacionado com o caráter informacional dessa nova economia, bem como no processamento de dados (CASTELLS, 2016, p. 176), sendo o processamento de dados exponencialmente sofisticado com a revolução tecnológica e, sobretudo, com o surgimento da Internet, elevando a velocidade no processamento e facilitando operações como transferência, compartilhamento, entre outros.

Por outro lado, Zuboff (2020, p. 20) adota um viés pouco mais pessimista em relação ao novo capitalismo que se erigiu, haja vista que, para a autora, “a realidade digital está tomando conta e redefinindo tudo que é familiar, antes mesmo de termos tido a chance de ponderar e decidir sobre a situação”. É nessa seara que a autora afirmará o seu conceito de capitalismo de vigilância, no qual tem “a experiência humana como matéria-prima para a tradução em dados comportamentais” (ZUBOFF, 2020, p. 18).

Além da mudança na forma econômica das empresas, naquilo que se conceituou como empresa em rede, o incremento das novas tecnologias no processamento de dados evidenciou uma nova forma de atuação mercadológica, não apenas na produção de dispositivos informáticos, na indústria microeletrônica, entre outros. Essa nova forma, como antes referido, está pautada no processamento de dados pelas empresas, *sítes* de comércio eletrônico e a gama de provedores ligados à Internet. Desponta, atualmente, a noção de Internet das Coisas, cujos aparelhos, em sua maioria domésticos, se utilizam da captação de dados pessoais para sua execução e aperfeiçoamento, que são ligados à Internet.

Como acentuam Marques e Lemos (2017, p. 11), Internet das Coisas “é uma rede na qual objetos físicos são instrumentalizados com sensores e ganham capacidades infocomunicacionais”, afirmando, por outro lado, que diversas questões

de segurança, privacidade e dados pessoais se erigiram a partir de então “desde a definição do tipo de dado captado pelos sensores, passando por suas formas de circulação e armazenamento, pelo compartilhamento com empresas parceira, pela relação com outros dados em banco de dados, pela interface de configuração de preferências pessoais” (MARQUES; LEMOS, 2017, p. 12). Contudo, como toda a tecnologia que envolve, ela pode trazer benefícios e malefícios. Magrani (2018, p. 24) sintetiza muito bem as contraposições existentes nessa tecnologia:

Sistemas de automação residencial permitirão que um consumidor, antes mesmo de chegar à sua residência, possa enviar mensagem para que os próprios dispositivos realizem ações para abrir os portões, desligar alarmes, preparar o banho quente, colocar música ambiente e alterar a temperatura da casa.

Por outro lado, esses numerosos dispositivos conectados que nos acompanharão rotineiramente irão coletar, transmitir, armazenar e compartilhar uma quantidade enorme de dados, muitos deles estritamente particulares e mesmo íntimos. Com o aumento exponencial de utilização desses dispositivos que já existem ou que entrarão em breve no mercado, devemos estar atentos aos riscos que isso pode acarretar para a privacidade e a segurança dos usuários.

Castells aponta, ainda em 2003, para o caráter fundamental dos dados no desenvolvimento do comércio eletrônico, eis que a principal fonte de renda advém da publicidade e do marketing, proporcionado por maciça utilização de dados pessoais (CASTELLS, 2003, p. 143). A ampliação da tecnologia trouxe como consequência imediata a crença de que a internet era um ambiente neutro e seguro (SARLET; CALDEIRA, 2019, p. 02), posto que, na mesma medida de seu desenvolvimento, seu uso se democratizou, ampliando a gama de usuários, facilitando o comércio (principalmente o eletrônico), o acesso à informação e, pode-se afirmar, a participação democrática.

No entanto, Castells, trabalhando a partir de uma lógica de vigilância da rede, alerta que “o entusiasmo com a liberdade trazida pela Internet foi tamanho que esquecemos a persistência de práticas autoritárias de vigilância” (CASTELLS, 2003, p. 143). Essa vigilância foi fartamente trabalhada pelos estudos do italiano Stefano Rodotà, a partir da constatação da maciça utilização dos dados pessoais dos cidadãos por entidades públicas e privadas, sem que a eles seja possibilitado algum controle (RODOTÀ, 2008, p. 36), o que, segundo o autor, exigiria uma nova perspectiva sobre a questão dos dados pessoais.

Nesse sentido, sobressaem os diversos mecanismos violadores dos direitos

das pessoas no ambiente digital, em razão de práticas que afetam os usuários gerando inúmeros riscos a quem utiliza a Internet. Dentre eles, há especial ênfase aos mecanismos de vigilância, sistemas algorítmicos e *profiling* que mitigam o acesso aos conteúdos dispostos na rede, bem como as questões que envolvem o consentimento na operação de dados pessoais por controladores, eis que o ato de consentir é expressão da liberdade na internet, além da gama de questões envolvendo a captação de superávit comportamental e da própria segmentação de comportamentos no ambiente digital.

Doneda exemplifica essa referida sofisticação citando a técnica do *profiling*, que consiste na utilização de inteligência artificial para se obter uma metainformação a partir de todas as informações coletadas e manipuladas do usuário de determinado serviço, podendo-se dela inferir diversas dimensões privadas e pessoais de quem o utiliza (DONEDA, 2019, p. 151). Dessa maneira, a Internet que foi desenvolvida e aprimorada a partir de um ideal de liberdade e colaboração científica, pouco a pouco também foi utilizada para outras finalidades, como a comercial que, a depender da oportunidade, não evidencia os mesmo ideais que a desenvolveram.

Apesar disso, a Internet também acarretou inúmeras mudanças positivas, que não podem ser colocadas em cheque. É inegável, por outro lado, que a forma com a qual vem sendo utilizadas as plataformas tecnológicas traz evidentes riscos, tanto sociais como individuais, e devem ser ponderados diante das realidades sociais. Como o próprio autor pontua (CASTELLS, 2003, p. 226) “a infraestrutura das redes pode ter donos, o acesso a elas pode ser controlado e seu uso pode ser influenciado, se não monopolizado”, deixando evidente que “a questão de quem possui e controla o acesso a ela dá lugar a uma batalha essencial pela liberdade”.

Dessa maneira, o presente trabalho, como já referido, busca compreender como a contínua, e por vezes irrestrita, utilização de dados pessoais dos usuários pode constituir impeditivo e restrição à liberdade dos usuários, acarretando possíveis riscos aos indivíduos que utilizam da rede, principalmente aos direitos fundamentais. Nesse sentido, imperiosa é, nesse momento, uma abordagem a partir do que propõem os estudos sobre a Sociedade de Risco e, após, como a estruturação social em forma de Redes na Internet e sua conseqüente exploração econômica pode ser fator gerador de riscos.

## **1.2 A Sociedade de Risco: entre as incertezas da modernidade reflexiva e os riscos globais**

Semelhantemente à Sociedade em Rede, as contribuições da Sociedade de Risco pretendem trazer uma compreensão a um determinado período histórico, que são teorizados em momento semelhante. Contudo, a proposta teórica parte principalmente sobre situações envolvendo riscos biológicos, ecológicos, nucleares, etc, em relação à tecnologia, e não a partir da evolução tecnológica e o surgimento da informática, como pretende Castells a partir da Sociedade em Rede. A Sociedade de Risco diz respeito à pós-modernidade, à era pós-industrial, pois, como afirmou Ulrich Beck (2011, p. 11), sobre o prefixo “pós”, que ele “é a palavra-chave de nossa época”.

Apesar de tal teoria não partir, como dito, do fenômeno da informação, as considerações trazidas com a Sociedade de Risco possuem importantes elementos coesivos com a Sociedade em Rede e a Era da Informação e de como elas podem potencializar riscos. Assim, permite uma ampla e multifacetada compreensão sobre o campo sociológico no qual se inserem os objetivos da presente pesquisa, quais sejam os dados pessoais e a liberdade na sociedade da informação. Todavia, antes de se adentrar nesses elementos coesivos, importa realizar um panorama sobre a Sociedade de Risco e sua proposta teórica.

De antemão, a perspectiva teórica da Sociedade de Risco possui determinados enfoques conferidos por autores diferentes. Apesar da convergência teórica, o recorte de estudo dos escritos é diferente, sendo possível enumerar dois enfoques ditos essenciais, conforme enuncia Aller (2006, p. 27), sendo Ulrich Beck caracterizado a partir de um tipo institucional, trabalhando por uma ótica da modernidade reflexiva da política, ciência e tecnologia, e de Niklas Luhmann a partir da teoria dos sistemas, não se olvidando a contribuição de Giddens, sob o enfoque fenomenológico. Como anteriormente já pontuado, a preferência aqui é pelos escritos de Beck, na medida em que a sua contribuição teórica, que também se volta à tecnologia, possibilita o aprofundamento do tema.

A Sociedade de Riscos é tratada como uma sociedade de incertezas, haja vista que “se está permeado por riscos desconhecidos e danos incontrolláveis, em que preponderam incertezas das consequências oriundas do meio científico e tecnológico” (BAGATINI, 2018, p. 22). Leal (2017, p. 41) argumenta que

nesta Sociedade de Riscos a ideia que guiava a Modernidade, qual seja, a de ser possível o controle dos efeitos colaterais e das decisões do homem restou em crise, razão pela qual Beck a define como uma sociedade do não-saber, porque no estágio alcançado pelo desenvolvimento tecnológico, os limites de controlabilidade dos riscos não tem se mostrado suficientes para evitar os danos que se consomem cada vez mais; ao contrário, cada aumento de saber/conhecimento/técnica tende a coincidir com o surgimento de novos riscos.

Erigida a partir do período posterior ao fenômeno da industrialização, a pós-modernidade, e também da própria pós-industrialização, Beck nomina existência dessa Sociedade de Riscos. Na época dos primeiros escritos de Beck, conforme ele mesmo afirmava, visualizavam-se indicativos de uma transição para o desenvolvimento dessa sociedade, haja vista que afirma que “encontramo-nos – esta é a minha tese –, pelo menos desde os anos setenta, no início dessa transição. [...] Ainda não vivemos numa sociedade de risco, mas tampouco somente em meio a conflitos distributivos das sociedades da escassez” (BECK, 2011, p. 25), demonstrando a existência de um período intermediário entre a Era Industrial e a Sociedade de Risco.

Nesse sentido, Machado e Guimarães (2017, p. 03) pontuam que a “teoria da sociedade de risco na pós-modernidade apresenta uma relação entre os processos de globalização dos riscos ecológicos e as manifestações específicas que estes podem adquirir em diferentes sociedades”. Contudo, o discurso de Beck não apenas se limita aos riscos ecológicos, podendo ser utilizado para compreensão da tecnologia e seus impactos sociais.

O uso do prefixo “pós” é muito presente em teorias que buscam compreender os fenômenos atuais, notadamente em razão de ser um período posterior à era da industrialização e da própria modernidade, muito presente na proposta teórica de Beck. Nesse sentido, afirma Germán Aller (2006, p. 23) que “la sociedad industrial del riesgo proviene de una fractura de la modernidad post sociedad industrial y la sociedad del riesgo es consecuencia de la obsoleto de la industrial”. Logo, é o processo histórico posterior à modernidade e da industrialização, com suas respectivas fraturas, que marca o início das mudanças sociais marcadas pela existência de riscos, pois, conforme Beck (2011, p. 12-13)

[...] 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 nova configuração social.

Nesse sentido, é preciso caracterizar o que se definem, para Beck, os riscos. Em um de seus textos, afirma que (BECK, 2000, p. 10) “los riesgos no aluden a daños acontecidos. No equivalen a destrucción. [...] No obstante, los riesgos amenazan con la destrucción”, ou seja, não são a destruição ou os danos em si, mas a possibilidade de eles existirem e se manifestarem dentro de um determinado contexto. Para Beck (2011, p. 31), “riscos, assim como riquezas, são objeto de distribuição, constituindo igualmente posições – posições de *ameaça* ou posições de *classe*” [grifo do autor].

Necessário também se fazer uma distinção entre perigos e riscos, pois conforme explica Aller (2006, p. 21), “en la actualidad hay riesgos casi incontrolables. En este aspecto, Beck distingue los peligros, que provienen de la naturaleza, y los riesgos, que son creados por el hombre”. Riscos e perigos, portanto, são diferentes e devem ser tratados de forma diferente, pois perigos são oriundos das questões da natureza, ao passo que os riscos são criados a partir da atividade humana.

Quando se fala em riscos, observa-se que esses, além de não serem igualmente distribuídos, são também desconhecidos a longo prazo (BECK, 2011) e que, com a modernidade, passaram a assumir um caráter global, ocasionando a existência de situações de ameaça global, diversamente do sentido de que os riscos possuíam em períodos históricos anteriores (BECK, 2011, p. 25).

Além disso, as ameaças e os riscos típicos de nossa época, “diferenciam-se, portanto, de seus equivalentes medievais, com frequência semelhantes por fora, fundamentalmente por conta da globalidade de seu alcance (ser humano fauna, flora) e de suas causas” (BECK, 2011, p. 27). Então, os riscos e ameaças daquela época eram diversos, haja vista que atualmente eles se proliferam a partir do avanço da ciência e de seu uso, como, por exemplo, na utilização de herbicidas nas plantações e sua relação com a proliferação das doenças, o que não estava na pauta dos riscos medievais. Nessa esteira, com a globalização e a globalidade também não se pode visualizar os riscos da mesma maneira que se visualizavam os riscos no medievo, por exemplo, dado o abismo tecnológico existente entre as duas épocas.

Com isso, Niklas Luhmann afirma que “en nuestros dias el concepto de riesgo aparece en las especialidades científicas más diversas e inclusive en las ciencias más variadas” (LUHMANN, 2006, p. 5), evidenciando que o risco também ocorre em diversas instâncias científicas, conforme igualmente propõe Ulrich Beck. Aliás, o avanço científico e tecnológico são as causas da potencialização dos riscos globais, a partir das transformações oriundas da sociedade industrial. Nesse sentido, afirma Machado:

A teoria da sociedade mundial do risco parece nascer com a percepção social dos riscos tecnológicos globais e de seu processo de surgimento até então despercebido. É uma teoria política sobre as mudanças estruturais da sociedade industrial e, ao mesmo tempo, sobre o conhecimento da modernidade, que faz com que a sociedade se torne crítica de seu próprio desenvolvimento. (MACHADO, 2005, p. 31)

No mesmo sentido, Machado e Guimarães (2017, p. 06) ressaltam que a teoria da Sociedade de Risco apresenta um conceito sobre a “nova modernidade (Pós-Modernidade), que opera mudanças drásticas na política, na economia e no comportamento, na medida em que a produção social de riquezas se faz acompanhar, cada vez mais, de uma produção social de riscos”. Alude Aller (2006, p. 26) que a Sociedade de Risco diz respeito a “una característica del desarrollo de la sociedad moderna que exhibe la dinámica de la creación de riesgos de diversos órdenes: políticos, colectivos, individuales, ecológicos y seguridad entre otros, que escapan al control social contemporáneo”.

A concepção de modernidade ocupa grande espaço na teoria, haja vista a distinção necessária entre o que o autor alemão denomina como modernidade simples e modernidade reflexiva. A modernidade simples seria aquela ocorrida no período industrial, enquanto que a modernidade reflexiva seria a própria Sociedade de Risco, surgida posteriormente à era da industrialização.

No entanto, Bagatini (2018, p. 23-24) pontua que a “sociedade de risco emergiu sob a égide e proteção da sociedade industrial. Os riscos fugiram ao controle desta sociedade, surgindo riscos sociais, políticos e econômicos, que hoje desafiam suas próprias instituições”, sendo tal constatação também afirmada por Leal (2017, p. 93), quando aduz que “nessa Sociedade, os riscos sociais, políticos e econômicos tendem a escapar do controle institucional ordinário do Estado. As próprias instituições privadas e de mercado começam a criar riscos que não podem

tampouco controlar”. Ainda, Bagatini (2018, p. 27) ressalta que “a sociedade de risco não foi um fenômeno buscado pelo ser humano, mas sim, uma consequência da modernização”.

Um ponto de destaque é acerca do caráter global dos riscos e também da própria globalização, uma vez que “os riscos destes cenários de pós-modernidade possuem tendência imanente à globalização, eis que acompanha a produção industrial um universalismo de perigos, independentemente dos lugares de sua produção” (LEAL, 2017, p. 45). Riscos, mesmo que se produzidos localmente, possuem uma tendência a atingir um caráter global, não se limitando ao espaço territorial e fronteiras. Há, então, uma ampliação dos riscos da modernização, relativizando-se as diferenças e fronteiras existentes (BECK, 2011, p. 43).

Aller, nesse contexto, aduz que “la globalización no es un hecho bueno ni malo *per se*, sino una forma de concebir a la sociedad cual si fuere una macro sociedad” (ALLER, 2006, p. 4). Contudo, é verdade que a globalização é produtora de riscos, impulsionando-os a atingir o caráter global, haja vista que Aller também afirma que, a partir dela, “los problemas y soluciones se van generalizando, tornándose cada vez más de corte colectivo em vez de individual y, al mismo tiempo, las decisiones involucran a múltiples comunidades; por ende, abarcan millones de personas más” (ALLER, 2006, p. 4), sendo que o contexto coletivo impõe uma distribuição de riscos e uma ampliação deles.

Apesar de haver uma distribuição de riscos com uma lógica diversa da distribuição de riquezas, as “sociedades de risco simplesmente não são sociedades de classes” (BECK, 2011, p. 43), possuindo uma inerente tendência à globalização e a um “universalismo das ameaças” (BECK, 2011, p. 43). Leal (2017, p. 45) exemplifica essa tendência à globalização dos riscos e universalismo das ameaças referindo sobre “os processos de contaminação das cadeias alimentarias em nível planetário, o problema das chuvas ácidas atacando prédios, obras de artes, plantações, lagos, dentre outros”, trazendo a evidência que os riscos podem, facilmente, atingir níveis globais.

Nesse contexto é que se insere a noção de efeito bumerangue dos riscos produzidos, mesmo diante de um padrão de sua distribuição<sup>8</sup>. Beck (2011, p. 44)

---

<sup>8</sup> A noção do efeito bumerangue é aplicável às questões relativas aos dados pessoais e a Internet, pois inúmeras fontes geradoras de riscos são também vitimadas pelos efeitos dos perigos que elas próprias produziram. Veja-se, por exemplo, os grandes bancos de dados ou mesmo os segredos

afirma que “nem os ricos e poderosos estão seguros diante deles [...] Os atores da modernização acabam, inevitável e bastante concretamente, entrando na ciranda dos perigos que eles próprios desencadeiam e com os quais lucram”.

Refere Aller (2006, p. 23), sobre o efeito bumerangue, que ele “destroza el esquema de clases, porque los riesgos se expanden y se acumulan [...], apareciendo un destino adscriptivo de peligro del que no hay aparente manera de escapar”. Ou seja, mesmo os atores sociais responsáveis pela criação/produção dos riscos estão suscetíveis de serem atingidos pelos riscos que eles mesmos criaram, posto que na Sociedade de Risco, as classes, apesar de serem responsáveis pela sua produção, são aniquiladas, demonstrando um efeito igualador no tocante às consequências.

Tais efeitos, como aduz Beck (2011, p. 45), não necessariamente podem atingir diretamente a vida ou a saúde dos seus responsáveis, mas podem atingir outros setores como o dinheiro, a propriedade e a legitimação, exemplificando que “o desmatamento causa não apenas o desaparecimento de espécies inteiras de pássaros, mas também reduz o valor econômico da propriedade da floresta e da terra” (BECK, 2011, p. 45). Conforme Leal (2017, p. 50), “vai-se reproduzindo retroalimentação entre danos que engendra espirais de destruição gradativa, fazendo com que se constitua uma sociedade amedrontada globalmente”. Dessa forma, não apenas diretamente os riscos causam prejuízos, mas, indiretamente, também afetam os bens humanos, ocasionando efeitos irrecuperáveis.

O nominado efeito bumerangue independe da localização da produção de risco e do atingido inicial de seus efeitos, haja vista que, nessa concepção, o risco, cedo ou tarde, poderá atingir o seu emissor, evidenciando o caráter global dos riscos. Reforça-se, nesse sentido, que os riscos possuem uma dimensão global, “em que os danos deles oriundos não são ou serão um fenômeno delimitado, sendo que todas as descobertas, triunfos e catástrofes afetam todo o planeta e não mais uma ordem local, nem mesmo um tempo específico” (BAGATINI, 2018, p. 24).

Vale dizer que, além do caráter global dos riscos, os danos desencadeados pelos riscos produzidos podem ser irreversíveis e invisíveis, baseando-se em interpretações causais, fazendo com que “instrumentos e posições de definição dos riscos tornam-se posições-chave em termos sociopolíticos” (BECK, 2011, p. 27). Aliás,

---

governamentais, cujos riscos de vazamento são prementes e, quando se transformam em danos, atingem até mesmo os seus produtores.

na medida em que são produzidos determinados riscos, partem eles para esfera da decisão política dos riscos e, conseqüentemente, ao Estado. Como aduz Bagatini (2018, p. 27):

O risco é inerente à modernidade, e o Estado, que financia e apoia o desenvolvimento da ciência e da tecnologia, ainda não oferece à sociedade respostas eficientes a uma série de novas demandas resultantes dessa modernidade. O Estado tem o dever de proteger o indivíduo (normalmente consumidor) desses riscos, de preferência anteriormente à ocorrência de um dano, mas como por vezes é deveras difícil, deve dar aparato à ressarcibilidade destes danos.

Nesse contexto, a Internet potencializou o surgimento de determinados danos oriundos de riscos produzidos, a exemplo de vazamentos e acidentes envolvendo grandes bancos de dados pessoais, fazendo com que seja incumbido o Estado a um dever estatal de proteger os indivíduos desses danos ocasionados, a partir da existência de um direito fundamental de proteção de dados pessoais, por exemplo, como será abordado nos capítulos seguintes. Além disso, imperiosa é também a execução de políticas para proteção da pessoa nessa seara e na criação de legislações protetivas que minimizem os riscos e danos que podem ocorrer.

Com a mudança da modernidade e dos próprios riscos originados a partir da modernidade reflexiva, o modo como tem sido buscado o controle dos riscos não tem se mostrado devidamente eficiente para evitar e prevenir os danos decorrentes de tais riscos (LEAL, 2017, p. 41), fazendo-se necessária uma reorganização/recontextualização das instituições e do Estado para se administrar tais riscos. Todavia, Leal (2017, p. 48) afirma que

A atual fase da modernidade não substitui simplesmente os princípios organizativos da Sociedade sob o ponto de vista da territorialidade, da coletividade e dos limites de competências do Estado-Nação, mas cria novas sinergias de coexistência entre estes e os novos paradigmas da chamada segunda modernidade, ordenada a partir da ideia de coordenação sistêmica entre globalização e individualização com o fito de estabelecer certos quadros conceituais como os de Estado, Lei, Políticas e Direitos Individuais re-conceitualizados.

Portanto, a modernidade não apenas elevou a categoria dos riscos, mas demonstrou a necessidade de se reconceitualizar determinados conceitos a partir dos novos riscos gerados. Nesse sentido, Beck (2011, p. 57) afirma que “a sociedade de risco dispõe, nessa medida, de novas fontes de conflito e de

consenso”, referindo, a partir de um paralelo com a sociedade erigida em classes, como a sociedade industrial, que “enquanto as sociedades de classes são organizáveis em Estados Nacionais, as sociedades de risco fazem emergir ‘comunhões de ameaça’ objetivas, que em última instância somente podem ser abarcadas no marco da sociedade global” (BECK, 2011, p, 57), novamente sendo demonstrado o caráter global dos riscos existentes. Nesse ponto, nota-se, no magistério de Leal (2017, p. 46), que

[...] a *globalização* se evidencia em face dos processos pelos quais os Estados Nacionais soberanos se misturam e se sobrepõem mediante atores transnacionais e suas respectivas probabilidades de poder. Assim, o conceito de globalização vem descrito como um processo que cria vínculos e espaços sociais transnacionais, revaloriza culturas locais e traz em primeiro plano outras culturas [grifo do autor]

Leal também afirma que a lógica dessa globalização e da globalidade não constituem fatores alheios às situações, devendo ser analisadas como oriundos das próprias relações existentes, impondo, na verdade, não a completa extinção dos riscos, mas uma forma maneira de geri-los diante desse contexto (LEAL, 2017, p. 46). Veja-se, portanto, uma mudança na perspectiva sobre a Sociedade de Risco, cujos indicativos são presentes na nossa modernidade, não se pretendendo que os riscos não existam ou sejam de pronto anulados, pois talvez constitua tarefa impossível, mas, na verdade, que sejam administrados adequadamente tais riscos de modo a possibilitar uma convivência com eles.

Nesse sentido, Ulrich Beck também propõe a noção de metamorfose digital, fenômeno que, para o autor, difere de uma revolução, considerando que diz respeito a efeitos colaterais que não foram intencionados pelos indivíduos, fazendo surgir a ligação entre os ambientes online e off-line (BECK, 2018, p. 190). Tudo isso, conforme Beck, faz com que os riscos globais se emancipem com os efeitos colaterais e, mais, fazem a expectativa de um humanismo digital, cuja base é a proteção dos dados pessoais e os direitos de liberdade diante do fato de que as pessoas são considerados dados em um oceano de dados (BECK, 2018, p. 190-192). Portanto, a metamorfose difere da revolução, pois essas modificações sociais não foram planejadas ou intencionadas, mas foram, simplesmente, ocorrendo.

O caráter global, a forma de controle dos riscos, a existência das ameaças, o próprio efeito bumerangue, são, portanto, marcas da Sociedade de Risco, não se

podendo evitar a existência deles, aliados à noção de metamorfose digital. Nesse sentido, apesar de que tal teoria, a partir dos escritos de Beck, é precipuamente baseada nos riscos ecológicos associados aos avanços científicos e tecnológicos, existem elos que coincidem com a própria teoria da Sociedade em Rede, anteriormente vista, e com o avanço tecnológico associado com a Internet, informática, microeletrônica, entre outros típicos da também nominada sociedade da informação.

Tais aspectos serão trabalhados no momento seguinte, buscando analisar detidamente de que maneira a Internet produz determinados riscos e danos que podem ocorrer, especialmente aos indivíduos que a utilizam, para que se possa compreender o fenômeno social em que se está inserido o Direito, sobretudo os direitos fundamentais e sua ligação com a Internet.

### **1.3 A Rede como Risco: a Era da Informação e os riscos da Internet**

A Sociedade em Rede, a partir da atual Era da Informação e do surgimento da Internet, no modo como anteriormente delineado, se constitui como uma Sociedade de Risco. Como visto, a Sociedade de Risco se manifesta na evidente incerteza nos riscos e perigos sociais, em uma sociedade de não conhecimento e não saber, pois “no estágio alcançado pelo desenvolvimento tecnológico, os limites de controlabilidade dos riscos não tem se mostrado suficientes para evitar que os danos que se consumam cada vez mais” (LEAL, 2017, p. 41).

Com a Internet, esses riscos se potencializaram, possibilitando atingir direitos do indivíduo nesse ambiente, com reflexos na vida e no cotidiano das pessoas. Obviamente, não se pode olvidar que as duas construções teóricas partem de perspectivas diferentes e se desenvolvem em distintas perspectivas para fornecerem as suas conclusões. Nesse sentido, assevera Fernandes acerca de importante aspecto temporal sobre as duas teorias, quando afirma, comentando a obra de Beck, que

A falta de ênfase na sociedade em rede – notória quando comparada com trabalhos como o de Castells – resulta, desde logo, do facto de o conceito de “sociedade de risco” ser anterior à expansão da internet para fora dos meios académico e militar e ao surgimento da sociedade em rede. Recordar-se que o conceito de “sociedade de risco” foi pela primeira vez proposto em 1986, em língua alemã, ainda no contexto da político-

ideológico da Guerra Fria. Ganhou posteriormente uma ampla difusão, a partir de 1992, com a sua tradução e publicação em língua inglesa, agora já num contexto de pós-Guerra Fria e de globalização em marcha (FERNANDES, 2013, p. 274).

Vale lembrar que foi no período da Guerra-Fria que a Internet pouco a pouco foi se firmando, popularizando-se apenas na década de 1990, demonstrando que a compreensão da sociedade como uma rede, conforme leciona Castells, é posterior às primeiras teorizações de Beck. Falbo e Keller (2015, p. 1996) aduzem ainda que

O argumento de Beck é construído com base no reconhecimento da transição entre a sociedade de classes e a sociedade de risco em curso na Alemanha desde os anos setenta do século XX. Neste sentido, haveria um período intermediário, nebuloso, em que elementos empíricos já confirmariam a nova configuração social em formação, sem que este quadro social importasse a eliminação definitiva da estrutura da sociedade de classes ainda existente.

No entanto, apesar da questão temporal existente, haja vista que os escritos de Beck precedem os de Castells, é possível visualizar elementos coesivos em ambas as teorias que possibilitam uma conclusão interessante sobre o fenômeno social, eis que, ao final, tratam de semelhante momento histórico, qual seja a ampliação da tecnologia, especialmente a partir da Revolução Industrial (mais marcadamente com a teoria de Beck), da Segunda Guerra Mundial e da ampliação da comunicação em caráter global, o que será adiante visto.

Além disso, apesar de ambas se referirem a semelhante período histórico, vale destacar, de acordo com Masi, que existem mais de trezentas conceituações usadas para denominar o atual momento (MASI, 2003, p. 33), sendo possível enunciar: modernidade reflexiva, modernidade líquida, sociedade pós-industrial, sociedade informacional, pós-modernidade, sociedade da informação, entre tantos outros. Não se ignora a existência dessas e de tantas outras conceituações igualmente importantes e bem delimitadas para a compreensão.

Todavia, o presente estudo buscou utilizar dois conceitos que objetivam compreender e explicar o fenômeno social e determinado período histórico, haja vista a convergência para a temática estudada, quais sejam os direitos fundamentais na sociedade da informação, principalmente se levado em conta o aspecto da Internet e as mudanças sociais por ela proporcionadas. Dessa maneira, especialmente os fenômenos decorrentes do avanço tecnológico, surgimento da informática e da Internet, por exemplo, podem apresentar convergências teóricas

para a posterior análise dos direitos fundamentais em nossa sociedade.

Nesse sentido, Bagatini apresenta um elo sobre os riscos da sociedade da informação, agregando aos riscos a noção de espetáculo, trabalhada pelo escritor francês Guy Debord, quando afirma que

A sociedade de risco, entendida como momento histórico atual, que se prolonga desde o início do século XX, com a queda do muro de Berlim e o fim da Guerra Fria, é compreendida como uma sociedade de incertezas, potencializada pela sociedade da informação, norteadada pelo espetáculo. A internet e, notadamente, as redes sociais mostra-se mecanismos de transmissão de informação, baseados no espetáculo, e acabam proliferando os riscos sociais (BAGATINI, 2018, p. 20-21).

Ou seja, a partir da consagração da transmissão da informação como ponto central da nova constituição social erigida com a informática e a Internet, aliada a uma possível incerteza social, é possível concluir que se proliferaram certos riscos. Doneda também argumenta que a imprevisibilidade dos tempos atuais é característica marcante, cuja incerteza pode se visualizar a partir da perspectiva do risco, conforme proposto por Beck (DONEDA, 2019, p. 52).

Nesse sentido, aduz que a lógica da Sociedade de Risco, a partir do conceito de risco, possui características próprias, pois “criado voluntariamente pela ação do homem, a decisão de produzi-lo não depende de considerações éticas ou morais, porém de um mecanismo decisional fortemente induzido pela tecnologia” (DONEDA, 2019, p. 52), aduzindo o autor que, dessa maneira, eliminar-se-ia “a importância de considerações particularizadas e tornando próprio risco algo impessoal, dissociado da ação humana” (DONEDA, 2019, p. 2). Veja-se, então que, para Doneda

tal discurso parece adequado à tecnologia: sua lógica não costuma ser a da pessoa individualmente considerada, visto que os custos e os meios de produção envolvidos requerem volume para que seja viável; portanto, podemos dizer que esse sistema funciona tendo em vista basicamente grandes números – dentro dos quais estão diluídos os indivíduos (DONEDA, 2019, p. 52)

Em síntese, verifica-se que a ampliação das tecnologias, marcadamente a Internet e a informática (aliadas às outras inovações a elas conectadas, quais sejam a microeletrônica, transmissão de dados, comércio eletrônico, entre outras), são fatores que impulsionam riscos. No entanto, para o aprofundamento da afirmativa,

deve-se passar pelo conceito de Sociedade em Rede. Assim, é pontual a lição de Fernandes (2013, p. 275), que, diga-se, trabalha a partir de uma lógica utópica dos dois modelos sociais propostos, quando afirma que

A referida ideia de risco e de sociedade de risco de Beck pode ser aplicada à sociedade em rede, na medida em que esta assenta numa criação tecnológica da modernidade reflexiva. O progresso tecnológico que permitiu a sociedade em rede – com todos os imensos benefícios que daí resultaram –, trouxe consigo uma nova área de risco para as sociedades humanas, consequência paradoxal (inevitável?) do seu sucesso.

Inevitável é que inúmeros riscos foram erigidos a partir da Internet e da constituição de redes. A exacerbada vigilância estatal, sob o fundamento do combate ao terrorismo, por exemplo, a vigilância dos grandes conglomerados empresariais da tecnologia, a chamada economia de dados, podem ser alguns exemplos dos riscos que a tecnologia proporcionou. Esses riscos estão diretamente atrelados ao desenvolvimento da Sociedade em Rede, que tem a tecnologia como seu vetor de impulso.

Nesse sentido, Castells afirma que “uma sociedade em rede é uma sociedade cuja estrutura social é construída em torno de redes ativadas por tecnologias de comunicação e de informação processadas digitalmente e baseadas na microeletrônica” (CASTELLS, 2019, p. 70), sendo ela “construída em torno de redes pessoais e organizacionais movidas por redes digitais e comunicadas através da internet e de outras redes de computadores” (CASTELLS, 2019, p. 37).

As incertezas e a incontabilidade causadas pelas inovações tecnológicas podem decorrer do maciço aumento de sua utilização passando a trazer, por exemplo, mudanças no conceito de privacidade, evidenciando riscos de violação dessa privacidade pela possibilidade de uso indevido dessas informações (FINKLESTEIN; FINKELSTEIN, 2019, p. 285), acarretando modificações também na esfera da liberdade dos indivíduos. Veja-se que essa maciça tecnologia desenvolvida na e pela Internet impossibilita o pleno controle dos riscos das consequências geradas, possibilitando o surgimento de novos riscos.

Evidencia-se isso, por exemplo, por diversos vazamentos de dados e informações, ataques informáticos, entre outros, que, além de não serem controlados pelo indivíduo, coloca-o em um campo de incertezas na utilização da tecnologia, dado que se trata de riscos invisíveis, o que se agrava com uma

deficitária proteção jurídica. Logo, considerando que “na sociedade de risco, a lógica é de natureza invertida, e o risco, invisível, muitas vezes. É o fato de os riscos poderem não ser percebidos que explica o florescimento, o crescimento e o fortalecimento dos mesmos” (FALBO; KELLER, 2015, p. 2000).

Nesse sentido, há um elo firmemente presente na sociedade de risco e na própria era moderna entre complexidade, contingência e informação. Leal (2017, p. 56) destaca que

a Sociedade do Risco é a Sociedade Moderna em estado latente de transformação, em toda a complexidade que pode ser compreendida enquanto fenômeno mais do que fatos e atos (individuais, coletivos e difusos), decorrente da correlação irrefreável entre contingência, complexidade e informação.

A informação, dentro do processo histórico do surgimento da informática, organizou-se em redes, haja vista que “como tendência histórica, as funções e os processos dominantes na era da informação estão cada vez mais organizados em torno de redes” (CASTELLS, 2016, p. 553).

Além disso, o fator global é ponto fulcral quando se fala nas constituições sociais de Rede e Riscos. Castells chega a tratar o fenômeno da globalização quase como sinônimo de sua teoria da Sociedade em Rede quando afirma que ao que “chamamos globalização é outra maneira de nos referirmos à sociedade em rede, ainda que de forma mais descritiva e menos analítica do que o conceito de sociedade em rede implica” (CASTELLS, 2005, p. 18). Do mesmo modo, Beck afirma que, na modernidade reflexiva, os riscos possuem uma tendência a um caráter global.

Porém, há uma diferenciação em Beck que deve ser pontuada nos conceitos de globalidade e globalização, que possuem características próprias. Segundo Leal (2017, p. 44), a globalidade se constituiria pelo fato de que “se vive em uma sociedade mundial em que quase inexistem espaços fechados de ação ou reação social ou institucional”. Essa globalidade possuiria algumas características (LEAL, 2017, p. 44-45), que seriam “certa *deslocalização* de causas e conseqüências de atos e fatos individuais e sociais, porque esses não se limitam a um único âmbito” [grifo do autor]; “incalculabilidade das conseqüências devido fundamentalmente aos

limites de conhecimento dos riscos contemporâneos”<sup>9</sup>; “não compensabilidade de danos que colocam em crise o princípio da segurança”. Acrescenta Leal que

essa globalidade nos faz dar conta de que nada que ocorre no planeta pode ser tido como algo local, regional ou nacional, eis que as novas descobertas tecnológicas e científicas, os desastres e catástrofes ambientais e industriais, afetam todo o mundo, razão pela qual devemos reorientar e reorganizar nossas vidas, assim como nossas instituições, tendo presente as relações inexoráveis do local x global (LEAL, 2017, p. 45).

Destaca-se que a globalização é fenômeno diferente na ótica da Sociedade de Riscos, uma vez que se materializa nas intersecções entre os Estados nas estruturas de poder, sendo ela descrita como “um processo que cria vínculos e espaços sociais transnacionais, revaloriza culturas locais e traz em primeiro plano outras culturas” (LEAL, 2017, p. 46). Nesse sentido, o paradigma da Sociedade em Rede demonstra a ampliação das redes de um modo local para um modo global, da mesma forma como a globalidade para Beck, evidenciando a reorganização individual e institucional.

Os nós constituídos a partir de diferentes locais foram capazes de formalizar a rede do modo como hoje é visualizada. Castells, assim, verifica que o fator global das redes foi determinante para a mudança da esfera de poder e da comunicação, haja vista que

o processo de formação e exercício das relações de poder é transformado de forma decisiva no novo contexto organizacional e tecnológico que se origina no surgimento de redes digitais globais de comunicação como o sistema fundamental de processamento de símbolos da nossa era. Portanto, a análise das relações de poder exige uma compreensão da especificidade das formas e processos da comunicação socializada - o que na sociedade em rede significa tanto a mídia de massa multimodal e as redes de comunicação horizontais e interativas, que têm como base a internet e a comunicação sem fio (CASTELLS, 2019, p. 22)

Entretanto, apesar de afirmar que a “estrutura social cuja infraestrutura esteja baseada em redes digitais tem a capacidade potencial de ser global”, e de concluir, então, que “a sociedade em rede é uma sociedade global” (CASTELLS, 2019, p. 71), a rede não obteve, ainda, sucesso de incluir todos em seus nós, apesar de que “todos são afetados pelos processos que ocorrem nas redes globais que

---

<sup>9</sup> Aliás, para Beck, o conhecimento dos riscos é primordial, pois “somente com o passo dado na direção da consciência de risco civilizacional é que pensamento e representação cotidianos se libertam das ancoragens no mundo das coisas visíveis” (BECK, 2011, p. 90)

constituem a estrutura social” (CASTELLS, 2019, p. 71). Dentro disso, Castells faz uma breve consideração acerca do local e do global das redes, notadamente quando afirma que todos têm as consequências dos processos das redes, especialmente aos que são externos a elas, afirmando que “o global supera o local” (CASTELLS, 2019, p. 72).

Assim como, para Beck, a nova modernidade trouxe crises e uma necessidade de reorganização, Castells se filia à afirmação de crise do Estado-Nação como entidade soberana, declarando, por outro lado, que “os Estado-Nação, apesar de suas crises em diversas dimensões, não desaparecem; eles se transformam para se adaptar a um novo contexto” (CASTELLS, 2019, p. 85).

Em paralelo, assim como a modernidade reflexiva trouxe a necessidade de adequadamente gestionar os riscos existentes a partir da pós-industrialização, que possuem um imanente caráter global, o conceito de Sociedade em Rede, aplicado ao âmbito estatal, também demonstra uma necessidade de transformação e gestão. Essa importância do Estado reside no fato de que globalização e globalidade levam em conta a necessidade de uma mudança de perspectiva sobre o Estado, especialmente diante da transnacionalização e da equação global x local, aplicados à teoria dos riscos.

Nesse sentido, diversas formas de manifestação da Sociedade em Rede, nos moldes daquela surgida pela Internet, são geradoras de risco. Fernandes (2013, p. 283) refere que

O progresso científico-tecnológico que permitiu a sociedade em rede trouxe consigo uma nova área de risco para as sociedades humanas, consequência paradoxal, e talvez inevitável, do seu próprio sucesso. A ideia de sociedade de risco de Beck capta bem essa realidade na atual sociedade em rede. Assim, é inequívoco estarmos perante mais um risco da modernidade reflexiva, o qual acresce ao catálogo de outros já bem conhecidos e diagnosticados, como o risco ecológico. Olhando retrospectivamente, é fácil constatar que nos criadores da internet e nos teorizadores dos primeiros tempos da sociedade em rede, o otimismo era a nota dominante, como se verifica na teorização dos anos 90 de Castells.

Contudo, tal otimismo e o ideal marcante da liberdade que guiaram os rumos da Internet não frearam o surgimento de riscos que, pouco a pouco, também vão se constituindo em danos, praticados seja por particulares, corporações e também os Estados-Nação. O desenvolvimento de uma nova economia, baseada em uma forma própria de capitalismo, fez surgir essas consequências, ao que Castells pontua a

necessidade, ainda em 2003, de enfrentamento de uma sensação de desconforto:

No início da Era da Informação, podemos perceber por todo o mundo uma extraordinária sensação de desconforto com os processos atuais de mudança conduzida pela tecnologia, que ameaçam gerar um efeito bumerangue generalizado. A menos que enfrentemos essa sensação, sua exacerbação poderá de fato destruir as promessas dessa nova economia e dessa nova sociedade nascidas da engenhosidade tecnológica e da criatividade cultural (CASTELLS, 2003, p. 225).

Engenhosidade tecnológica e criatividade cultural que, ao lado da ideia de liberdade, foram os motores da chegada Internet, como antes já referido. Porém, tais motores, a essa altura, passadas quase duas décadas da afirmativa de Castells, foram obnubilados e deram espaço a uma massiva produção de riscos e danos consequentes a eles. Dentre exemplos, é possível citar os rotineiros vazamentos de dados pessoais ocasionados por falhas de segurança, ataques cibernéticos entre outros; carência de transparência política, mesmo diante da ampliação dos espaços democráticos proporcionados pela rede; a vigilância em massa praticada por corporações e pelos Estados.

Aliás, sobre o último aspecto, Fernandes (2013, p. 277) argumenta que “há uma tendência dos governos, a qual não ocorre apenas nos Estados autoritários, de vigiar os hábitos dos seus cidadãos *online*”. Referido autor ainda levanta importante questão sobre como essa vigilância em massa deve ser enfrentada pelos sistemas jurídicos, sobretudo a partir do fenômeno global, afirmando que “tais mecanismos de controle e vigilância dos Estados poderão ser considerado uma violação dos direitos inerentes ao ser humano na era da sociedade em rede” (FERNANDES, 2013, p. 277), levantando a questão sobre os direitos humanos eletrônicos (ou digitais, como também podem ser chamados). Além disso, referido autor manifesta grande preocupação com os riscos existentes naquilo que ele intitula de ciberguerra, haja vista que se trata de “um risco que tem vindo a aumentar, pela crescente dependência da economia e da sociedade das redes informáticas e de telecomunicações” (FERNANDES, 2013, p. 284).

Dentre tantos exemplos de como a Rede potencializou riscos partir dos mecanismos de vigilância, ocasionando uma verdadeira devassa à privacidade das pessoas e de seus dados, talvez os relativos às consequências na esfera privada dos atentados de 11 de setembro de 2011 e ao site *Wikileaks*, ambos nos Estados Unidos, se sobressaem, ainda mais se considerados os direitos à privacidade e à

liberdade envolvidos nas duas situações.

Especialmente se levado em conta o ideal de liberdade presente desde o início da construção da Rede pela Internet, pois afirma Castells que “a Internet é de fato uma tecnologia da liberdade – mas pode libertar os poderosos para oprimir os desinformados, pode levar à exclusão dos desvalorizados pelos conquistadores do valor” (CASTELLS, 2003, p. 225). Nesse contexto, corporações e os Estados visualizaram promissores instrumentos para ampliação de seus negócios e dos controles, com base nessa nova forma de comunicação, posto que

conforme a internet se expandia para se tornar o principal meio de comunicação na era digital, as grandes corporações passaram a dominar o seu negócio, e as companhias de telecomunicações globais moldaram as plataformas móveis de comunicação. Como este livro discute, a principal forma organizacional de comunicação na era digital é representada por redes de negócios multimídia globais com formas diferentes de comunicação reunidas no mesmo conglomerado e com alta concorrência em um ambiente de negócios cada vez mais oligopolista (CASTELLS, 2019, p. 30).

Leal (2020, p. 362) afirma que, em geral, é possível terceiros conhecerem os hábitos de outros, o que prescinde de suas vontades, uma vez que “boa parte de nossa vida passa e se dá – direta e indiretamente – por vias digitais, transmitindo dados e informações que não sabemos como são gerenciados”. Em síntese, diversos são os riscos e danos que podem existir nesse ambiente típico da atual forma da Sociedade em Rede, baseada em redes digitais através da Internet.

Valorosa parte deles ocorre com fins econômicos e de controle: elaboração de perfis de consumo, violações às privacidades e direitos individuais, além de riscos democráticos, a exemplo das denominadas *fake news*, notícias de caráter falso, muitas vezes disseminadas a partir da combinação algorítmica. Rodotà faz um alerta necessário quando se combina Internet e os indivíduos, afirmando que ela e suas transformações “devem permanecer disponíveis para permitir a livre formação da personalidade, o exercício da liberdade de expressão e de associação o desenvolvimento de iniciativas cívicas, a experimentação de novas formas de democracia (RODOTÀ, 2008, p. 158)

Distante da pretensão de alarmismo sobre o modo como os elementos Internet, privacidade, dados pessoais, além da própria democracia, proliferam riscos, fato é que há uma grande mudança de perspectiva no modo de se fazer negócios, política, gerir Estados, obter acesso a informações, entre outras situações

cotidianas, e que, como os estudos acadêmicos demonstram, se utilizam de mecanismos violadores, geradores de riscos e perigos aos indivíduos. Leal, nesse sentido, apresenta interessante contraponto entre a privacidade e os interesses mercadológicos presentes nesses novos mecanismos:

Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infundáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos (LEAL, 2020, p. 366).

É possível realizar um paralelo com a noção de liberdade na Internet e da própria neutralidade da rede, na medida em que se encontram descoladas de seu sentido inicial. Sabido é que a Internet modificou a soberania dos Estados e o controle que estes antes tinham sobre as informações, uma vez que transcende as fronteiras dos Estados, não sendo possível a eles, como faziam ao longo da história, ser o centro de controle das informações e do poder (CASTELLS, 2003, p. 140).

Ademais, diante desse contexto, a fim de retomar as tecnologias de controle e de vigilância que anteriormente possuíam, “os governos desenvolveram seus próprios programas de vigilância, combinando desajeitados métodos tradicionais com nova sofisticação tecnológica” (CASTELLS, 2003, p. 145), possibilitando amplo acesso às informações. Leal (2020, p. 361) ainda argumenta que “também os países europeus têm intervindo e modo ainda mais incisivo na privacidade e intimidade das pessoas físicas e jurídicas, e em contextos caracterizados pelos mais elevados níveis de tecnologia e informação”, citando o exemplo francês e um Estado de Exceção a partir dos atentados yihadistas no país.

Do mesmo modo, o destaque é conferido às empresas privadas, especialmente as redes sociais, que ascenderam de forma exponencial nos últimos tempos, utilizando-se das informações como mercado, o que é exemplificado por Leal quando afirma que “todo o ‘curtir’ ou registro feito por meio do Facebook gera informações que são analisadas e classificadas por algoritmos [...], desenvolvendo modelos sociais para agências de publicidade, o que gera milhões de dólares para a empresa” (LEAL, 2020, p. 362).

Além disso, Castells pontua como a liberdade foi solapada pelos governos e

também pelas empresas precursoras dos ideais de liberdade na Internet quando afirma:

A ironia é que, em geral, foram as firmas da Internet, de ideologia ardorosamente libertária, que forneceram a tecnologia para a quebra do anonimato e a redução da privacidade, e foram as primeiras a usá-la. Assim fazendo, deixaram a vigilância do governo voltar a rugir com furor redobrado no espaço de liberdade que fora laboriosamente construído pelos pioneiros da Internet, tirando proveito da indiferença ignorante das burocracias tradicionais (CASTELLS, 2003, p. 147).

Aliado a isso, há uma crescente concentração da propriedade dos meios de comunicação, além da variedade de ofertas das plataformas digitais (CASTELLS, 2019, p. 122), o que faz crescer uma centralização ainda maior das informações e dos dados, acarretando, por consequência, uma maior produção dos riscos da Internet.

Nesse sentido, Zuboff trabalha a partir da importância que as empresas relacionadas à Internet tiveram, fazendo surgir uma nova forma de capitalismo, que ela denomina como capitalismo de vigilância, que é “uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vender” (ZUBOFF, 2020, p. 9).

Além disso, Zuboff (2020, p. 17), a partir desse conceito, traz importante exemplo da maciça vigilância e violação de dados e informações, além da segurança, com o caso do termostato Nest, capaz de coletar inúmeros dados pessoais de seu usuário a partir de sofisticada inteligência artificial, possibilitando armazenamento de dados, depósitos de conhecimento e poder, assumindo a empresa responsável pouca responsabilidade pela segurança.

A autora aponta sérias consequências ao ser humano, haja vista que, nessa forma de capitalismo, a experiência humana é a matéria-prima, permitindo mapeamento de dados comportamentais, ampliação do mercado de comportamentos futuros, bem como a automatização das pessoas (ZUBOFF, 2020, p. 18-19), acarretando inúmeros riscos e consequências ao ser humano e a sua liberdade nesse ambiente de vigilância constante.

Além disso, acrescenta a autora que

Essa nova forma de mercado é uma lógica de acumulação única na qual a vigilância é um mecanismo fundacional na transformação de investimento em lucro. Sua rápida ascensão, a elaboração institucional e a

significativa expansão desafiavam a promessa incerta de inversão e seus valores orientados para a proteção. De forma mais geral, a ascensão do capitalismo de vigilância traía as esperanças e expectativas de muitos “*netizens*” [cidadãos da net] que louvaram a promessa emancipatória do meio conectado em rede (ZUBOFF, 2020, p. 69).

Essa traição às promessas é visível, segundo a autora, na história da empresa Google, pois “desde o começo, a empresa personificava a promessa do capitalismo de informação como uma força social democrática e libertadora que animava e encantava populações da segunda modernidade ao redor do mundo” (ZUBOFF, 2020, p. 85). Entretanto, pouco a pouco a empresa passaria a ser a maior capitalista de vigilância a partir da captação de dados do superávit comportamental dos usuários, caracterizando, para a autora, a principal das empresas responsáveis por essa nova forma de mercado (ZUBOFF, 2020, p. 27). Em outra oportunidade, a autora expressa amiúde o crescimento da empresa:

A Google tornou-se a maior e mais bem-sucedida empresa de *big data* por ter o site mais visitado e, portanto, possuir a maior quantidade de *data exhaust*. Como muitas outras empresas digitais, a Google correu para atender às ondas de demanda reprimida que inundaram a esfera individual em rede nos primeiros anos da *world wide web*. Era um exemplo claro de empoderamento individual nas demandas de uma vida mais eficaz. Mas, à medida que as pressões para o lucro avançavam, os líderes da Google se preocupavam com os efeitos que o modelo de serviços pagos poderia ter no crescimento do número de usuários. Eles então optaram por um modelo de propaganda. A nova abordagem dependia da aquisição de dados de usuários como matéria-prima para análise e produção de algoritmos que poderiam vender e segmentar a publicidade por meio de um modelo de leilão exclusivo, com precisão e sucesso cada vez maiores. À medida que as receitas da Google cresciam rapidamente, aumentava a motivação para uma coleta de dados cada vez mais abrangente. A nova ciência de análise de *big data* explodiu, impulsionada em grande parte pelo sucesso retumbante da Google (ZUBOFF, 2018, p. 32).

Assim, denota-se que as críticas da autora são contundentes e muito bem fundamentadas para traçar o panorama histórico e econômico dessa nova modalidade de mercado geradora de intensos riscos.

Decorre desse contexto que os ordenamentos jurídicos, cada vez mais, especialmente as doutrinas internacionais, vão buscando uma maior regulamentação e ampliação das esferas de proteção, haja vista que as relações entre as pessoas e as sociedades ocorrem no seio das novas tecnologias (LEAL, 2020, p. 365).

Entretanto, Zuboff lança o alerta para essas novas previsões normativas,

pois, para ela, questões como o consentimento são facilmente transponíveis por parte desses novos agentes do mercado, haja vista que, além da possibilidade de alteração unilateral das políticas de privacidade, por exemplo, tratam-se de contratos de adesão, onde não há espaço para diálogo acerca do tratamento conferido à privacidade e dados pessoais (ZUBOFF, 2020, p. 64-65). Apesar da quase unanimidade dos teóricos em declarar que o Estado se encontra em crise, é justamente necessário que se reorganize e busque uma adequada proteção e gestão dos riscos, que se proliferam de modo global.

A partir disso é que Fernandes conclui ser a Sociedade em Rede uma utopia, enquanto que a Sociedade de Risco uma realidade, haja vista que a teoria de Castells, em verdade, restou solapada pelos riscos e danos que a Internet possibilitou gerar. Nas palavras do autor:

Olhando retrospectivamente, é fácil constatar que nos criadores da internet e nos teorizadores dos primeiros tempos da sociedade em rede, o otimismo era a nota dominante, como se verifica na teorização dos anos 90 de Castells. Todavia, a utopia da sociedade em rede tornou-se uma realidade, mas não exatamente como os ideais tecno-libertários julgavam ser possível. Em parte isto ocorreu porque o mundo económico-empresarial se apropriou desta, submetendo-a às regras do mercado e da produção capitalista, ou seja, subvertendo o ideal comunitário de partilha e de colaboração numa base não lucrativa. Em parte ocorreu também porque a internet e a *web* se tornaram um espaço que mimetiza a complexidade da natureza humana (FERNANDES, 2013, p. 283-284).

Dessa maneira, direitos fundamentais são amplamente afetados nessas perspectivas, com especial destaque aos direitos da privacidade e de liberdade das pessoas, pois, diante da Sociedade em Rede visualizada como uma Sociedade de Risco, passam a assumir uma nova concepção. Essas modificações oriundas da modernidade reflexiva aliada ao modo como Internet imposta atualmente nossas vidas, impõe uma nova maneira de gestionar os riscos existentes em nossa atual sociedade, notadamente pela figura do Estado.

Esse modo de gestão de riscos não implica a busca pela extinção total dos riscos, pois, aqui, acarretaria, em última instância, a completa extinção das novas tecnologias e dos avanços existentes, por exemplo, além de grandes ferramentas que foram criadas, como o comércio eletrônico, que já estão consolidadas no seio da sociedade. Na verdade, há que se minimizar os seus efeitos, notadamente os riscos extraordinários, gerindo-os de uma maneira que pode ser considerada adequada para a proteção dos indivíduos diante desses riscos. Ou seja,

exemplificativamente, não se poderia pretender acabar com o tratamento de dados pessoais, o controle estatal de determinadas maneiras, entre outros, bastando apenas equacionar tais práticas de modo a não acarretar graves riscos e danos aos indivíduos.

Nesse sentido, uma maneira prática dessa equação no âmbito estatal é através da via legislativa, seja ordinária ou constitucional, de modo a conferir uma adequada proteção e segurança aos indivíduos, com vistas a gerir os riscos existentes nessa modernidade erigida pela Internet e de prevenir eventuais danos decorrentes de violações à privacidade, aos dados pessoais, à liberdade. Conforme adiante será exposto, para se conferir uma suficiente proteção jurídica, sobretudo com patamar constitucional, são necessárias transformações nos ordenamentos jurídicos, a exemplo da que será trabalhada no presente trabalho, qual seja um direito fundamental à proteção de dados pessoais, autônomo à privacidade, bem como de medidas legislativas ordinárias como forma de tutelar a liberdade no ambiente digital.

## **2. DIREITOS FUNDAMENTAIS E INTERNET: LIBERDADE E PRIVACIDADE FRENTE AOS RISCOS DA REDE**

No capítulo anterior, abordou-se o panorama teórico em que se encontra inserida a discussão pretendida no presente trabalho, qual seja o da Sociedade de Risco a partir da criação das tecnologias informáticas, geradoras de riscos e perigos à pessoa e aos direitos fundamentais nesse ambiente. O debate que se fará neste segundo momento é analisar os elementos que os tradicionais direitos de liberdade e de privacidade enfrentam para a tutela jurídica da pessoa no ambiente digital diante do panorama da Sociedade de Risco.

Nesse sentido, em um primeiro momento será brevemente analisada a teoria dos direitos fundamentais e os principais conceitos para compreensão da temática proposta na presente dissertação, inserindo o debate no seio da teoria da Sociedade de Risco, bem como do panorama do ambiente digital. A partir disso, buscar-se-á analisar como a Internet possibilita a mutação da leitura dos direitos fundamentais, gerando novas vertentes teóricas, a exemplo do constitucionalismo digital.

Posteriormente, será realizado um percurso teórico a partir do direito fundamental à liberdade e os novos contornos que ele assume na Era da Informação. Para isso, necessário se partir das questões elementares sobre tal direito, que assumiu e assume notável importância na história, agora, se mostrando mitigado frente alguns instrumentos das tecnologias da informação. Após, analisar-se-á o direito à privacidade, a partir também das bases históricas e jurídicas necessárias, para visualizá-lo em um novo contexto e os evidentes riscos à privacidade diante do tratamento automatizado de dados e informações com os novos mecanismos digitais.

### **2.1 Breve excursão sobre a teoria dos direitos fundamentais na Constituição de 1988 e a Era da Informação**

Longe de pretender fazer tautologia, trazendo considerações sobre questões já assentadas na doutrina, a discussão proposta no presente subcapítulo é de demonstrar que os direitos fundamentais se modificaram ao longo do tempo, de modo a atender determinados anseios teóricos de cada momento histórico e verificar que, com a tecnologia informática e a internet, tal questão não está sendo diferente. Nesse sentido, denota-se que a transformação social impacta diretamente nas relações

jurídicas, sobretudo com a busca por liberdade e direitos. Como bem já apontou Bobbio

Não é preciso muita imaginação para prever que o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderão introduzir tais mudanças na organização da vida humana e das relações sociais, que se criem ocasiões para o nascimento de novos carecimentos e, portanto, para novas demandas de liberdade e de poderes (BOBBIO, 1992, p. 33).

Contudo, antes mesmo de adentrar nessa questão, é preciso resgatar os conceitos históricos basilares da teoria dos direitos fundamentais, fornecendo o necessário substrato para a análise de novos direitos fundamentais, como é o caso da proteção de dados pessoais, e de compreender a mudança de clássicos direitos, como a liberdade e a privacidade. Leal (2000, p. 33), quando trata sobre a perspectiva dos direitos humanos e o Estado, aduz que eles são produto da história, raciocínio que é aqui aplicável quando se fala de direitos fundamentais, não sendo possível deixar de fazer, mesmo que minimamente, este percurso.

Como visto anteriormente, as transformações oriundas daquilo que Castells chamou de Sociedade em Rede são acarretadoras de diversos riscos, o que, no nosso contexto, é nominado por Ulrich Beck como Sociedade de Risco. Essa sociedade apresenta diversas relações entre Estado e Risco, conseqüentemente, assumindo também uma imbricação entre a Sociedade de Risco e os direitos fundamentais. As modificações oriundas da modernidade reflexiva aliadas ao modo como Internet imposta atualmente nossas vidas, consoante anteriormente referido, impõem a reflexão de uma nova maneira de gestionar os riscos existentes em nossa atual sociedade, notadamente pela figura do Estado, a quem se direcionam os direitos fundamentais.

Ademais, a digressão teórica a ser aqui realizada sobre a base dos direitos fundamentais é importante também para se analisar possíveis controvérsias teóricas e de aplicação do direito fundamental na situação concreta. Conforme Vieira (2007, p. 55), quando trata da teoria dos direitos fundamentais para analisar a privacidade, a reflexão permite analisar

da aplicabilidade dessa garantia nas relações jurídicas privadas; do papel do Estado na conformação desse preceito; da possibilidade do indivíduo renunciar a esse direito nas relações jurídicas assimétricas; da possibilidade dos empregadores monitorarem as comunicações eletrônicas dos empre-

gados; da amplitude do âmbito de proteção desse direito fundamental; da extensão do sigilo de correspondência às comunicações por *e-mail*; da possibilidade de limitação do sigilo das comunicações e de correspondência dos presos sem autorização judicial (...)

Vale lembrar que a relação que existe entre o Estado e os direitos fundamentais é visível quando se analisa os modelos estatais e os direitos consagrados ao longo do tempo, dado que os direitos fundamentais historicamente forçaram a limitação do poder (SARLET, 2010, p. 36). Assim, a transformação estatal também é a evolução dos direitos fundamentais, sobretudo nos anseios pela ampliação das liberdades e mitigação dos poderes alheios, especialmente na figura do Estado.

É a partir da promulgação da Constituição da República Federativa de 1988 que se inaugura no Brasil, após longos anos de Estado autoritário, o Estado Democrático de Direito, fundamentado na dignidade da pessoa humana e lastreada em um amplo rol de direitos e garantias fundamentais. Nesse sentido, a Lei Maior de 1988 ampliou significativamente o rol de direitos e garantias fundamentais, sendo que, desde o seu preâmbulo, afirma a edificação de um Estado Democrático de Direito com objetivo de assegurar o exercício dos direitos fundamentais (BRASIL, 1988).

Contudo, para se chegar ao que se conhece hoje por direitos fundamentais, houve uma gradativa evolução das Constituições brasileira, desde a primeira Constituição, em 1824, até a atual, percorrendo extensas modificações no sistema de direitos fundamentais, que constituem direitos subjetivos e elementos básicos do Estado Democrático de Direito (LEAL, 2000, p. 187). Essa concepção perpassa pela conhecida história dos diversos modelos de Estado, a partir do Estado Liberal, do Social até o Democrático de Direito, no modo como os direitos fundamentais se perpetuaram em cada um deles, até a sua forma atual, onde se observa uma maior relevância dos direitos fundamentais e das normas constitucionais sobre as normas ordinárias, a partir da noção de eficácia de irradiação das normas constitucionais<sup>10</sup>.

Importa, inicialmente, delimitar um conceito de direito fundamental que servirá para a digressão teórica consequente do presente trabalho, notadamente porque o direito fundamental à proteção de dados pessoais, principal direito em debate neste trabalho, foi, por muito tempo, extraído materialmente da Constituição

---

<sup>10</sup> Importa aqui destacar que a irradiação das normas constitucionais é fenômeno decorrente do movimento do Constitucionalismo Contemporâneo, marcado pela observância dos direitos fundamentais e pela jurisdição constitucional.

brasileira, posto que não positivado<sup>11</sup>. Conforme Dimoulis e Martins (2018, p. 52) os direitos fundamentais são “direitos público-subjetivos de pessoas (físicas ou jurídicas), contidas em dispositivos constitucionais e, portanto, que encerram caráter normativo supremo dentro do Estado, tendo como finalidade limitar o exercício do poder estatal”, advogando, portanto, sob um aspecto mais positivo dos direitos fundamentais, entendendo que somente são fundamentais os direitos expressamente previstos na Constituição. Um elemento que se extrai desse conceito é a ideia dos direitos fundamentais como forma de limitação do exercício do poder estatal.

No ambiente da Era da Informação, com a massiva operação de informações e dados, não apenas o Estado possui enorme poder de impedir o exercício de direitos fundamentais, mas alguns atores privados igualmente assumiram poderio igual ou maior nesse aspecto, inclusive com o apoio do próprio Estado. Trata-se daquilo que Beck (2018, p. 188) nominou como poder digital central autônomo, controlador do âmbito privado através de meios democráticos. Todavia, as relações entre Estado e esses agentes econômicos privados e a fruição dos direitos fundamentais é um desafio da Era da Informação.

Sarlet, por outro lado, em seu conceito defende uma maior expansividade do rol dos direitos fundamentais, a qual o presente trabalho se filia, referindo sobre a possibilidade de direitos materialmente fundamentais, que não se encontram no corpo da Constituição (2017, p. 325), conceituando como direitos fundamentais

todas as posições jurídicas concernentes às pessoas (naturais ou jurídicas, consideradas na perspectiva individual ou transindividual) que, do ponto de vista do direito constitucional positivo, foram, expressa ou implicitamente, integradas à constituição e retiradas da esfera de disponibilidade dos poderes constituídos, bem como todas as posições jurídicas que, por seu conteúdo e significado, possam lhes ser equipadas, tendo, ou não, assento na constituição formal (SARLET; MARINONI, MITIDIERO, 2017, p. 323)

Decorre desse entendimento, a admissão de alguns direitos não positivados expressamente na Constituição, mas possuidores de mesmo status, como o caso da autodeterminação informativa e também da proteção de dados em certa medida, quando ainda não era expressamente positivada. Nesse sentido, independentemente do caráter dos direitos (se formal ou material) cada direito

---

<sup>11</sup> Todavia, recentemente, por meio da PEC 17/2019, mediante aprovação do Senado Federal, tal direito foi consagrado na Constituição, inserido no rol de direitos e garantias fundamentais do artigo 5º (BRASIL, 2019).

possui uma esfera de proteção própria e delimitada. A teoria dos direitos fundamentais divide, então, o estudo de cada direito fundamental em espécie em seu âmbito de proteção e os limites existentes para tal direito.

Como pontuam Dimoulis e Martins (2007, p. 132-133) “estudar os direitos fundamentais significa principalmente estudar suas limitações”, demonstrando a importância do estudo da temática quando se trata de direitos fundamentais. Nesse sentido, o âmbito de proteção é o bem jurídico tutelado por esse direito fundamental (SARLET, 2010, p. 387), ou seja, o objeto que o direito visa assegurar e proteger dentro de determinado aspecto. Por outro lado, os limites dos direitos fundamentais são as

ações ou omissões dos poderes públicos (Legislativo, Executivo e Judiciário) ou de particulares que dificultem, reduzam ou eliminem o acesso ao bem jurídico protegido, afetando o seu exercício (*aspecto subjetivo*) e/ou diminuindo deveres estatais de garantia e promoção (*aspecto objetivo*) que resultem dos direitos fundamentais (SARLET, 2010, p. 291).

Destaca-se, assim, que os direitos fundamentais “têm restrições limitadas e, tais limites, conforme a Constituição Federal, se referem tanto à necessidade da proteção de um núcleo essencial de direito fundamental, quanto à clareza, determinação, generalidade e proporcionalidade das restrições impostas” (LEAL, 2000, p. 187), surgindo o que a doutrina chama de princípio da proteção do núcleo essencial, que objetiva impedir restrições desprovidas e descabidas (LEAL, 2000, p. 187). Dimoulis e Martins (2018, p. 161), referem que “os limites aos direitos fundamentais apresentam possibilidades de condutas e situações que fazem parte da área de proteção do direito fundamental”, residindo a importância de se analisar ambas questões em conjunto e de conferir relevância no momento dos estudos, posto que “os direitos fundamentais tornam-se relevantes somente quando ocorre uma intervenção em seu livre exercício” (DIMOULIS; MARTINS, 2018, p. 153).

Para se falar em uma teoria geral dos direitos fundamentais, importa ainda traçar alguns aspectos acerca das suas dimensões (ou gerações, conforme parcela da doutrina pretende)<sup>12</sup>. Trata-se de teoria que visa, pedagogicamente, traçar um limite temporal para compreensão do aspecto evolutivo dos direitos fundamentais,

---

<sup>12</sup> No ponto, há que se fazer o importante destaque pela preferência do termo dimensões, a despeito das críticas de conhecimento notório. Sem adentrar no mérito, mas, como já referido por Sarlet (2010), linha à qual o presente trabalho se filia, o uso da palavra dimensões confere a noção de complementaridade necessária na evolução dos direitos fundamentais.

normalmente subdividido em três momentos distintos, dos quais não existem maiores divergências doutrinárias.

Virgílio Afonso da Silva aduz que a primeira geração/dimensão – utilizados pelo autor como sinônimos – diz respeito aos direitos de liberdade, especialmente contra o Estado, bem como aos direitos políticos (SILVA, 2005, p. 547). Já a segunda dimensão de direitos fundamentais trata de uma dimensão de direitos envolvendo ações positivas por parte do Estado, ligados aos ideais de igualdade material, surgindo os denominados direitos sociais (SARLET, 2010, p. 48). Por sua vez, a terceira dimensão de direitos ligados à fraternidade, consagrando uma titularidade difusa, tratada como indefinida (SARLET, 2010, p. 48-49), nos quais se encaixam os direitos à paz, autodeterminação dos povos, meio ambiente, entre outros.

Parcela da doutrina delimita uma quarta e quinta dimensão, decorrente de alguns novos direitos, nomeadamente os direitos relativos à Internet e da bioética. Tratam-se, todavia, de direitos que estão abrangidos, de algum modo, pelos eixos das outras dimensões ou são decorrentes deles. Como pontua Gorczewski (2016, p. 147), ao tratar sobre a evolução dos direitos humanos, não é preciso que, a cada novo fato relevante para a sociedade, que se faça surgir uma dimensão (ou geração) própria de direitos, com uma conseqüente fundamentação. Logo, denota-se que aquilo que se entende por uma nova geração de direitos acaba sendo abrangida por outras dimensões, não devendo se banalizar a teoria das dimensões na medida em que surgem novas proteções nessas searas.

Ainda acerca das dimensões, vale aqui lembrar a crítica de Marmelstein acerca da teoria das dimensões de direitos fundamentais, que não devem ser vistas sob um aspecto isolado, mas complementar. Nas palavras do autor:

O ideal é considerar que todos os direitos fundamentais podem ser analisados e compreendidos em múltiplas dimensões, ou seja, na dimensão individual-liberal (primeira dimensão), na dimensão social (segunda dimensão), na dimensão de solidariedade (terceira dimensão) [...] Não há qualquer hierarquia entre essas dimensões. Na verdade, elas fazem parte de uma mesma realidade dinâmica [...].

Veja-se, a título de exemplo, o direito à propriedade: na dimensão individual-liberal (primeira dimensão), a propriedade tem seu sentido tradicional, de natureza essencialmente privada, tal como protegida no Código Civil; já na sua acepção social (segunda dimensão), esse mesmo direito passa a ter uma conotação menos individualista, de modo que a noção de propriedade fica associada à ideia de função social (art. 5º, inc. XXIII, da CF/88); por fim, com a terceira dimensão, a propriedade não apenas deverá cumprir uma função social, mas também uma função

ambiental. (MARMELSTEIN, 2014, p. 53).

Dentro do panorama da teoria dos direitos fundamentais, deve-se fazer uma especial referência à dupla perspectiva dos direitos fundamentais, que dá surgimento as dimensões subjetiva e objetiva (que em nada se confundem com a teoria das dimensões vista acima). Sarlet (2010, p. 152) aduz que a dimensão subjetiva trata da possibilidade de que a um “titular de um direito fundamental é aberta a possibilidade de impor judicialmente seus interesses juridicamente tutelados perante o destinatário (obrigado)”.

Dimoulis e Martins (2018, p. 138) referem, por outro lado, que ela se trata de “um direito de seu titular de resistir à intervenção estatal em sua esfera de liberdade individual”. No entanto, na noção proposta por Sarlet, não somente o Estado é o destinatário dos direitos fundamentais, mas também os particulares podem figurar como destinatários, submetidos, portanto, à vinculação e observância dos direitos fundamentais (SARLET; MARINONI; MITIDIERO, 2017, p. 377).

Por outro lado, a dimensão objetiva surgiu mais recentemente, a partir da decisão do Tribunal Constitucional Alemão no caso *Lüth-Urteil*, que inaugurou a perspectiva dessa dimensão e a ideia de eficácia de irradiação dos direitos fundamentais (LEAL; MAAS, 2018, p. 51). Conforme comentam Maas e Leal:

Na prática, o Tribunal Constitucional Alemão implantou a ordem para que, nas relações privadas, entre particulares, seja em uma questão possessória, contratual ou de família, os direitos fundamentais também sejam observados, não se podendo conceber relações jurídicas (de qualquer natureza, e não apenas aquelas que envolvam diretamente os direitos fundamentais), à margem da Constituição, devendo o Estado zelar pela defesa dos direitos fundamentais não só nas relações em que é parte, mas, ainda, nas relações privadas. (LEAL, MAAS, 2018, p. 54-55).

A dimensão objetiva apresenta que “os direitos fundamentais passaram a apresentar-se, no âmbito da ordem constitucional, como um conjunto de valores objetivos básicos e fins diretivos da ação positiva dos poderes públicos” (SARLET; MARINONI, MITIDIERO, 2017, p. 351), evidenciando que os direitos fundamentais transcenderam a perspectiva subjetiva, por todos devendo ser observados, não apenas de modo passivo, mas observado ativamente por todos. Essa perspectiva surge da noção de eficácia de irradiação das normas constitucionais sobre as normas de direito privado, vinculando imediatamente o legislador de direito privado, como acentua Canaris (1937, p. 129-130).

No seio da noção de dimensão objetiva é que se insere a questão envolvendo os deveres de proteção do Estado ou imperativos de tutela. Apesar da crítica elaborada pelos autores Dimoulis e Martins (2018, p. 142), trazem sucinto conceito sobre o tema aduzindo que referido dever estatal se trata do “dever do Estado de proteger ativamente o direito fundamental contra ameaças de violação provenientes, sobretudo, de particulares”. Nesse sentido, “o dever de proteção envolve a atividade legislativa, administrativa e jurisdicional do Estado, e é um dos mais importantes desdobramentos da teoria contemporânea dos direitos fundamentais – dimensão objetiva” (KOHLS, LEAL, 2018 p. 158). Assim, aponta-se que

em virtude do aspecto objetivo dos direitos fundamentais, o Estado está obrigado a criar pressupostos fáticos necessários ao exercício efetivo desses direitos, como possui o dever de não apenas abster-se de intervir no âmbito de proteção a esses direitos, como também de proteger os mesmos contra agressões de terceiros (LEAL, MAAS, 2018, p. 60).

Acrescenta-se a isso que a dimensão objetiva representa a proteção dos bens mais especiais para a convivência e sociedade como fruto do princípio máximo da dignidade da pessoa humana, vinculando os entes públicos a perseguirem ativamente a defesa e proteção dos direitos (VIEIRA, 2007, p. 93). A concepção do dever estatal de tutela ganhará contornos práticos quando se referirá acerca do direito fundamental à proteção de dados pessoais, sobretudo diante da Era da Informação e das metamorfoses de riscos típicas da Sociedade de Risco.

A partir desse breve panorama sobre a teoria dos direitos fundamentais, é necessário fazer algumas considerações sobre os direitos fundamentais nesse novo ambiente, que é o ambiente digital, possibilitado a partir da difusão da informática e da Internet. Sobretudo, diante de um ambiente de metamorfose digital permitida pela Internet, nos termos pontuados por Beck (2018, p. 193), quais sejam a desconexão da proximidade geográfica e a proximidade social, o encurtamento da distância entre ficção e realidade e, principalmente, a incontabilidade do Estado-nação, com a proliferação de riscos e perigos da Sociedade de Risco.

É inegável que os fatores Internet e informática impulsionaram mudanças nas instituições e direitos, especialmente os direitos fundamentais. Nesse sentido, Landa (2016, p. 2) aponta que “en esta nueva etapa de transformación del Estado y la sociedad, el Internet es el fundamento principal para construir la nueva identidad

de los derechos fundamentales”.

A afirmação demonstra que não apenas surgiram novos direitos fundamentais a partir da escala que a Internet tomou, mas essas novas relações estão a fazer com que a própria teoria dos direitos fundamentais seja, de alguma maneira, metamorfoseada também, conferindo uma nova identidade aos direitos fundamentais. O autor ainda aponta que a Internet não apenas transformou a equação entre os direitos, mas também se tornou ela um direito fundamental quando permitiu às pessoas a possibilidade de usufruir dos direitos e liberdades clássicos, dessa vez em um ambiente digital (LANDA, 2019, p. 146).

No mesmo sentido, essa perspectiva de uma “releitura” dos direitos fundamentais perpassa sobre as questões basilares da teoria, mas a partir de novos modelos de proteção. É o que aponta Landa quando refere que

El desarrollo de nuevas tecnologías permite a las industrias de las telecomunicaciones y la informática desarrollar cada vez más sofisticados sistemas, programas y aparatos de vigilancia electrónica, los cuales demandan nuevos estándares de protección de los derechos fundamentales, para evitar que se cometan excesos que afecten tanto a terceros como a los investigados, salvo en los casos en que sea estrictamente necesario. En el caso de que se cometan excesos, deben existir mecanismos de control sobre los privados, no únicamente estatales, sino también desde la ciudadanía y/o sus representantes en el Estado, por cuanto la interceptación y el almacenamiento de datos de las comunicaciones privadas en la era digital constituyen un grave peligro para los ciudadanos e incluso para las autoridades (LANDA, 2019, p. 155).

Veja-se que algumas características próprias da Internet fazem com que a questão sobre direitos fundamentais deva ser analisada sob um prisma diferenciado. Importante exemplo é sobre a jurisdição constitucional diante de um ambiente digital desterritorializado e descentralizado como a Internet. Caso interessante e que demonstra essa perspectiva é a que vem sendo enfrentada pelo Supremo Tribunal Federal por meio da Ação Direta de Constitucionalidade nº 51, que versa sobre a obtenção de meios de prova de provedores de aplicação que coletam os dados de comunicação privada no Brasil, mas os armazenam nos Estados Unidos (BRASIL, 2017). Com o surgimento da rede nos Estados Unidos, onde também se encontra valorosa sede de provedores de aplicação (a exemplo do *Facebook*), e a expansão para as mais diversas partes do planeta, as operações envolvendo comunicação privada e dados se expandiram a nível global.

Nesse sentido, muito se tem discutido sobre a necessidade de observância

de acordos de assistência judiciária entre Estados (os mencionados MLAT's) para praticar determinados atos e diligências na esfera penal a partir de dados de comunicações privadas constantes em centros de dados situados em países estrangeiros, nos quais os Estados não estariam cobertos pela soberania. A divergência trata principalmente acerca da obtenção de meios de prova durante a persecução penal, mas tem os direitos fundamentais e a Internet como pano de fundo e ponto a ser enfrentado. Como apontam Guidi e Rezek:

Estados dividem-se em suas fronteiras, jurisdições se pretendem universais, mas são limitadas por outras igualmente vocacionadas, a “comunidade” internacional, conglomerado de Estados e Organizações aferradas a suas soberanias, tem um largo caminho a percorrer até atingir a mesma integração mundial que a Internet nos deu em pouco mais de duas décadas (GUIDI; REZEK, 2018, p. 277).

A questão tem sido controvertida nos tribunais brasileiros que ora utilizam o disposto no artigo 11 do Marco Civil da Internet, ora entendem ser necessária a utilização dos mecanismos de cooperação internacional. Nesse sentido, tem-se que o “intuito da ADC é que o Tribunal consolide o uso de acordos de cooperação mútua, em detrimento da aplicação do art. 11 do Marco Civil da Internet” (MENDES; FERNANDES, 2020, p. 25), tendo em vista que a obtenção dos dados era impedida pelo fundamento que a determinação judicial brasileira não seria aplicável nos Estados Unidos, pois coberta pela soberania estatal e de legislação diversa, que proibia o fornecimento das informações.

Assim, observa-se que “uma entidade estatal não tem como ordenar que determinado seja realizado dentro da esfera de outro Estado” (SILVA, 2019, p. 667). Percebe-se, então, que o conflito jurisdicional envolvendo os direitos fundamentais é complexo, uma vez que a privacidade dos usuários, a soberania, o poder punitivo estatal e a jurisdição estão em jogo na ADC nº. 51, cuja decisão de mérito ainda não foi tomada.

Observa-se disso que o panorama dos direitos fundamentais na Era da informação ainda é terreno arenoso diante das características próprias da Internet e da informática e demonstra ainda mais a dificuldade do Estado lidar com riscos próprios da Era da Informação, qual seja a coleta de dados, mesmo sendo ele um controlador dos dados, numa apontada contradição trazida por Beck (2018, p. 193). Uma solução apontada por Landa (2018, p. 3) é que a Internet impõe o cumprimento

dos compromissos internacionais. Nas palavras do autor:

en la medida que los derechos fundamentales son universales, interdependientes e indivisibles, el internet los integra digitalmente y permite que trasciendan más allá de las fronteras de los Estados nacionales; no solo para el goce del mismo, sino también para su defensa y protección. Lo cual demanda que los Estados cumplan con sus compromisos internacionales de garantizar y promover los derechos humanos, en esta nueva era digital (LANDA, 2018, p. 3).

Além disso, surgem no Direito algumas correntes que pretendem estudar e apontar soluções. Dentre elas, o nominado Constitucionalismo Digital vem como “uma corrente teórica do Direito Constitucional contemporâneo que se organiza a partir de prescrições normativas e comuns de reconhecimento, afirmação e proteção de direitos fundamentais no ciberespaço” (MENDES; FERNANDES, 2020, p. 5). Trata-se de movimento teórico que busca trazer contribuições as questões envolvendo Internet e direitos fundamentais. Nesse sentido, Mendes e Fernandes (2020, p. 6) trazem que

dentro dessa perspectiva, pressupõe-se que a fruição de direitos fundamentais pode ser mediada pela força impositiva do Estado Nacional, ainda que em convivência com modalidades outras de conformação de direitos que têm origem na atuação de agentes privados ou no funcionamento de mecanismos transnacionais de governança da internet.

Em síntese, entendem que a Internet possibilita a realização das garantias individuais e que ela também é necessária para que muitos direitos sejam adequadamente fruídos (MENDES; FERNANDES, 2020, p. 6). Nesse sentido, inúmeras propostas legislativas surgiram no Brasil, sendo o Marco Civil da Internet um dos principais no que diz respeito a normas que disciplinam a Internet, trazendo garantias de liberdade de expressão e pensamento, proteção à privacidade, desenvolvimento da personalidade (BRASIL, 2014), tidos também, direta ou indiretamente, como fundamentais pela Constituição, de modo a trazer algumas garantias mínimas nesse ambiente. Mendes e Fernandes (2020, p. 8) apontam que as iniciativas “consagram materialmente categorias de direitos, princípios e normas de governança para a internet, limitando drasticamente o poder de autoridades públicas e de atores privados nas suas relações com os usuários”.

Assim, a Internet é uma garantia institucional da democracia e uma necessidade para que se goze plenamente dos direitos e liberdades previstos na Constitui-

ção e também nos tratados sobre direitos humanos (LANDA, 2019, p. 146). Essa importância ainda é reforçada quando os direitos fundamentais são constantemente violados sem a plena consciência da sua violação por parte dos indivíduos afetados, como é o caso dos mecanismos de vigilância estatal e privada, afetando os direitos de privacidade, proteção de dados e também de liberdade nesse ambiente digital, no seio de uma forma de vida e de economia que já é presente na realidade humana, dificultando, de alguma forma, a balança entre as questões. Em um ambiente de riscos como a Internet, a devassa à liberdade se mostra fator de consumação de danos por vezes irreparáveis, como se verá adiante.

## **2.2 O direito fundamental à liberdade e seus novos contornos na Sociedade de Risco**

A partir da breve exposição antes realizada anteriormente é possível analisar especificamente o direito fundamental à liberdade. Em suma, pretende-se aprofundar o debate sobre a perspectiva teórica do direito para que se possa fazer o seu estudo diante do ambiente digital e da Sociedade de Risco, fornecendo substrato para analisá-lo diante desses cenários. Certamente, o direito fundamental à liberdade é bastante amplo, nomeadamente na aplicação das suas diversas espécies, sendo a exposição teórica sobre o direito em espécie realizada de modo sumário para que se possa fazer a análise proposta.

A liberdade talvez seja o mais abrangente dos direitos fundamentais e também aquele historicamente mais reivindicado, tendo em vista que abarca as mais diversas searas da expressão humana. Um dos primeiros documentos de direitos humanos de nossa era, qual seja a *Magna Carta*, de 1215 (Carta Magna das Liberdades), trouxe a liberdade como grande fator para a limitação do poder político diante do abusivo poder monárquico (COMPARATO, 2019, p. 83). Percebe-se que as primeiras reivindicações sobre a liberdade justamente diziam respeito a um tipo de afastamento da intervenção do poder estatal, ou seja, em um sentido negativo, para que o Estado deixasse de intervir na liberdade pessoal (o que também muito tem ligação com um conceito clássico de privacidade, que será abordado posteriormente). Mendes (1999, p. 2) entende que essa ideia geral de liberdade se vincula ao grupo dos chamados direitos de defesa:

A clássica concepção de matriz liberal-burguesa dos direitos fundamentais informa que tais direitos constituem, em primeiro plano, direitos de defesa do indivíduo contra ingerências do Estado em sua liberdade pessoal e propriedade. Esta concepção de direitos fundamentais – apesar de ser pacífico na doutrina o reconhecimento de diversas outras – ainda continua ocupando um lugar de destaque na aplicação dos direitos fundamentais. Esta concepção, sobretudo, objetiva a limitação do poder estatal a fim de assegurar ao indivíduo uma esfera de liberdade. Para tanto, outorga ao indivíduo um direito subjetivo que permite evitar interferências indevidas no âmbito de proteção do direito fundamental ou mesmo a eliminação de agressões que esteja sofrendo em sua esfera de autonomia pessoal.

Ou seja, seria a liberdade um direito que possibilitaria em larga escala a fruição dos demais direitos fundamentais. A história demonstra que essa concepção negativa, na ideia de não intervenção, pouco a pouco se mostrou insuficiente frente aos anseios sociais. As lutas pelos direitos consagraram, então, a ideia de que não bastava apenas o Estado se eximir de interferências, mas deveria agir positivamente para assegurar o exercício dos direitos, nomeadamente o direito de liberdade. Na concepção de Mendes:

Vinculados à concepção de que ao Estado incumbe, além da não-intervenção na esfera da liberdade pessoal dos indivíduos, garantida pelos direitos de defesa, a tarefa de colocar à disposição os meios materiais e implementar as condições fáticas que possibilitem o efetivo exercício das liberdades fundamentais, os direitos fundamentais a prestações objetivam, em última análise, a garantia não apenas da liberdade-autonomia (liberdade perante o Estado), mas também da liberdade por intermédio do Estado, partindo da premissa de que o indivíduo, no que concerne à conquista e manutenção de sua liberdade, depende em muito de uma postura ativa dos poderes públicos (MENDES, 1999, p. 3).

Dessa maneira, o exercício do direito de liberdade, dentro da evolução dos direitos fundamentais, foi um dos protagonistas na busca pela limitação do poder e consagração dos direitos individuais. Essa visão do direito de liberdade é fruto da tradicional visão dos direitos fundamentais, ligados a padrões de observação e pensamento, típica dos paradigmas liberais (ALBERS, 2016, p. 21). Essa concepção “como proteção contra violações de direitos ou ingerências neles parece ser uma proteção abrangente e ótima da liberdade” (ALBERS, 2016, p. 13), mas que sofre transformações diante da complexização social e jurídica decorrente de uma proteção de dados pessoais.

No Brasil, dentre o extenso rol de direitos previstos no artigo 5º da Constituição de 1988 - e também ao longo dela - há especial destaque ao direito

fundamental de liberdade, que a este busca proteger por diversas oportunidades e maneiras, considerando um elemento primordial da dignidade humana e pilar do Estado (MENDES; BRANCO, 2016, p. 242). Vinculada à noção de dignidade da pessoa, tem-se que “as liberdades são proclamadas partindo-se da perspectiva da pessoa humana como ser em busca da autorrealização, responsável pela escolha dos meios aptos para realizar as suas potencialidades” (MENDES; BRANCO, 2016, p. 242).

E nesse sentido é possível afirmar que a “Constituição Federal é, portanto, também e em primeira linha, uma constituição da liberdade” (SARLET; MARINONI; MITIDIERO, 2017, p. 484), encontrando-se ela como “condição de valor princípio e direito (mas também como dever)” (SARLET; MARINONI; MITIDIERO, 2017, p. 485). Trata-se, essencialmente, de um direito geral de liberdade, não apenas de um rol de liberdades em espécie, possibilitando um reforço normativo firme ao nível dos direitos fundamentais (SARLET; MARINONI, MITIDERO, 2017, p. 485), que é permitido a partir de uma concepção materialmente aberta dos direitos fundamentais.

Da leitura da Constituição da República de 1988, percebem-se as inúmeras referências ao direito de liberdade, inclusive como objetivo fundamental da República na constituição de uma sociedade livre (BRASIL, 1988). É no artigo 5º que se encontram as maiores referências a esse direito, quando se trata da ideia de um amplo direito de liberdade limitado apenas por lei, conforme o inciso I, ou como liberdade de manifestação do pensamento, na esteira do inciso IV, e de liberdade de locomoção, garantida, entre outros, pelo inciso XV (BRASIL, 1988).

Nesse sentido, na seara dos tratados internacionais e de direitos humanos a liberdade também assume importância notável nesses documentos. Uma das principais referências é a Declaração Universal dos Direitos Humanos, que resguarda a liberdade nos artigos, dentre outros, 1º, 2º e 3º (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948). Além disso, observa-se que a Convenção americana de Direitos Humanos também traz alguns postulados sobre o direito de liberdade, notadamente em seu artigo 7º (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969). Isso demonstra a importância assumida pelo direito de liberdade, seja em âmbito nacional como internacional, e a devida proteção que esse direito deve ter.

Para José Afonso da Silva (2017, p. 235), a liberdade seria a “possibilidade de coordenação consciente dos meios necessários à realização da felicidade

peçoal” e, nesse sentido, para o autor, se apresentaria em cinco grandes grupos na atual ordem constitucional: liberdade da pessoa física, liberdade de pensamento, liberdade de expressão coletiva, liberdade de ação profissional e liberdade de conteúdo econômico e social (SILVA, 2017, p. 237).

Outras possíveis classificações são trazidas pela doutrina a partir dos desdobramentos das espécies de liberdades previstas no texto da Constituição de 1988, frisando-se, porém, que a liberdade se trata também de um direito geral de liberdade, cujos limites apenas podem ser colocados mediante lei, observando-se o princípio da legalidade (SARLET; MARINONI, MITIDIERO, 2017, p. 486-488). Uma vez que a liberdade assume tamanha importância histórica, jurídica e política, suas restrições somente podem ocorrer mediante a observância do processo legislativo regrado pelo princípio da legalidade, de modo que qualquer impeditivo ao seu exercício pode configurar violação ao direito fundamental.

As liberdades, nesse sentido, possuem espécies próprias como, por exemplo, a liberdade de expressão, de locomoção, consciência, etc, que possuem âmbitos de proteção com conteúdos também próprios a partir da peculiaridade do direito em espécie, cujos limites também corresponderão ao direito em questão. Além disso, importante considerar que as disposições constitucionais acerca das liberdades possuem eficácia plena e são diretamente aplicáveis (SILVA, 2017, p. 270), especialmente considerando que esse direito fundamental tem ainda mais relevo em uma sociedade democrática, que é seu campo de exercício (SILVA, 2017, p. 236).

Considerando a proposta do presente estudo, as espécies de direitos de liberdade serão aqui estudados de modo exemplificativo, sempre tendo em mente o direito geral de liberdade, dado que, com a Internet, sofreram mudanças em suas formas de manifestação e também de violação. Com isso, é possível entender de que maneira essa nova formação social acarreta mudanças específicas no agir humano e, conseqüentemente, no exercício das liberdades.

O estudo da liberdade pessoal e de circulação no ambiente erigido a partir da difusão Internet permitirá uma análise profunda desses direitos dentro do contexto mencionado. Trata-se de um questionamento que Rodotà já fazia sobre como a liberdade de circulação se impostaria no ambiente digital, aliado a outras liberdades, como a de expressão e de associação, que serão indiretamente abordados (RODOTÀ, 2008, p. 200).

Veja-se que tal espécie toma duas frentes diferentes com o ambiente digital: seja por meio da vigilância constante, permeando a nossa liberdade, seja pela liberdade de circulação no interior da própria Internet. Além disso, será analisado o nominado direito ao livre desenvolvimento da personalidade, que apesar de estar relacionado ao rol dos direitos de personalidade, é “um direito de liberdade, no sentido de um direito de qualquer pessoa a não ser impedida de desenvolver sua própria personalidade e de se determinar de acordo com suas opções” (SARLET; MARINONI, MITIDIERO, 2017, p. 439), noção que também decorre da ampliação do direito de liberdade na Constituição.

Certamente, a questão sobre uma forma de liberdade de circulação na Internet traz inúmeros debates e reflexões. No entanto, se tomado em conta que a forma clássica desse direito não se visualiza suficiente para uma adequada proteção diante da formação de perfis informáticos, direcionamentos de conteúdo a partir da captação de superávit comportamental para segmentação comportamental da pessoa, por exemplo, é visível que o questionamento de Rodotà (2008, p. 200), a partir da Constituição Italiana, de “qual é o alcance da liberdade de circulação (art. 16) na presença da vigilância por vídeo e difusão das técnicas de localização?” e de se “as garantias da liberdade pessoal (art. 13) devem ser também estendidas ao corpo ‘eletrônico, seguindo a trajetória da releitura do *habeas corpus* como *habeas data*?” (grifo do autor), assume importância para debate na seara dos direitos fundamentais.

Os ativistas virtuais Julian Assange, Jacob Appelbaum, Andy Müller e Jérémie Zimmermann, em obra coletiva, trataram do tema liberdade de circulação com preocupação diante da massiva vigilância estatal. Para Assange, três liberdades são fundamentais, quais sejam a de comunicação, circulação e de interação econômica. Acrescenta-se a essa ideia, nas palavras do autor, que

Se olharmos para a transição da nossa sociedade global para a internet, quando fizemos essa transição a liberdade de circulação pessoal permaneceu basicamente inalterada. A liberdade de comunicação foi enormemente expandida em alguns aspectos, no sentido de que agora podemos nos comunicar com um número muito maior de pessoas; por outro lado, ela também foi enormemente reduzida, porque não temos mais privacidade e as nossas comunicações podem ser interceptadas, armazenadas e, como resultado, usadas contra nós. Então a interação elementar que temos fisicamente com as pessoas acabou se degradando (ASSANGE; *et al*, 2013, p. 89).

A liberdade de expressão, para eles, assumiu novos contornos diante das devassas à privacidade. Todavia, não somente nesse contexto, posto que a ampliação da possibilidade de expressão permitiu outras formas de violação a outros direitos. Conforme trazem Mendes e Fernandes (2020, p. 7), o aumento dos espaços de fala permitidos pela Internet “torna a liberdade um campo fértil para diversas formas de abusos, o que pode ser percebido na disseminação de discursos odiosos, *cyberbullying*, pornografia infantil e mesmo na difusão em massa de notícias falsas”.

Contudo, a linha adotada pelos ativistas virtuais trata nomeadamente da vigilância estatal e de riscos a ela associados. Nesse sentido, é plausível que a interceptação da comunicação privada realizada através da Internet ilegalmente afeta de alguma maneira o direito à liberdade de comunicação, tendo em vista que a inviolabilidade das comunicações privadas constitui uma garantia fundamental do cidadão (STRECK, 1997, p.17)<sup>13</sup>. Essa garantia, no ambiente digital, não se estende tão somente contra as violações estatais, mas também a causada por entes privados, nomeadamente agentes econômicos da Internet. Jacob Appelbaum acrescenta que, em verdade, os espaços de expressão no mundo real<sup>14</sup> também se viram limitados pelas restrições à liberdade de circulação, pois, nas palavras do autor,

Se formos seguir essa noção reducionista da liberdade, das três liberdades que Julian mencionou, isso é claramente vinculado à liberdade de circulação – hoje em dia não dá nem para comprar uma passagem de avião sem usar uma moeda rastreável, caso contrário a transação é imediatamente sinalizada. Se você entrar em um aeroporto e tentar comprar uma passagem para o mesmo dia com dinheiro vivo, você é imediatamente visado e será forçado a passar por revistas de segurança extra, não poderá voar sem identificação e, se tiver a infelicidade de comprar sua passagem

---

<sup>13</sup> Veja-se que, no Brasil, não existem grandes escândalos de interceptação de comunicações privadas, seja pelo ente estatal ou privado, como ocorreu no escândalo *Wikileaks*, tratando-se de questões muito mais pontuais. O fatídico escândalo *Wikileaks* trouxe à tona o modo como os Estados se utilizam do ambiente digital para promover indevidas vigilâncias, trazendo sérios riscos aos direitos fundamentais e humanos.

<sup>14</sup> Conforme Zuboff (2020, p. 16), em verdade, a questão entre a delimitação daquilo que pode ser considerado mundo real e mundo digital tende a ficar menor. É nítido que com a ascensão na utilização de *smartphones*, *smartwatch*, entre outros equipamentos, as fronteiras do digital cada vez mais consomem a nossa realidade. Trata-se daquilo que Zuboff (2020, p. 01) nomina como a era do capitalismo de vigilância, baseado na captação do superávit comportamental para práticas comerciais. A autora traz o exemplo do Termostato Nest, já visto brevemente no primeiro capítulo, capaz de não apenas trazer as informações típicas de um termostato, mas também de coletar dados de diversos outros produtos conectados a ele ou a Internet (ZUBOFF, 2020, p. 17). Põe-se em cheque a noção de que a residência é um espaço de liberdade, pois, com a ampliação das ferramentas *smart* (ou *smarthome*), ela acaba sofrendo restrições por terceiros.

com um cartão de crédito, eles registrarão tudo – desde o seu endereço IP até o seu navegador. (ASSANGE; *et al*, 2013, p. 99)

Se visualizada a teoria dos direitos fundamentais, sob a análise do direito de liberdade em espécie, verifica-se que a noção sobre a liberdade frente às tecnologias permite de uma releitura. Trata-se de direito que possui duas dimensões de seu âmbito de proteção. Em uma concepção subjetiva, é o direito de defesa de não se ver restringido na livre circulação e locomoção, sem que haja qualquer tipo de embaraço (SARLET; MARINONI; MITIDIERO, 2017, p. 527-528). De outro lado, a acepção objetiva é facilmente extraída a partir dos elementos de base antes visto, posto que se trata de um dever do Estado de assegurar o exercício desse direito de liberdade, garantindo os meios materiais para esse exercício.

Assim, sendo direito fundamental de suma importância, os novos riscos associados à Internet e novas tecnologias e a liberdade em específico exigem uma proteção maior e suficiente, tendo em vista que a violação da liberdade é diferente dos outros direitos fundamentais e dos riscos globais, uma vez que o risco a ela possui uma ameaça imaterial (BECK, 2018, p. 186). Essa proteção, na seara constitucional, perpassa por uma ampliação da materialização do dever de proteção estatal, por exemplo, através da via legislativa e atuação de autoridades voltadas à proteção desses direitos.

No Brasil, há uma proteção jurídica mínima para a liberdade no ambiente digital, como se verá adiante, principalmente com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, perpassando essa proteção por uma proteção de dados pessoais. Todavia, ela não se mostra atualmente suficiente<sup>15</sup>. A uma, pois o Brasil caminha a passos lentos para a compreensão da proteção aos direitos fundamentais no ambiente digital, bastando-se ver que a proteção em legislação iniciou a pouco mais de uma década e a morosidade na efetiva atuação da Autoridade Nacional de Proteção de Dados Pessoais, recentemente instituída. A duas, pois a Internet, a nível mundial, é regulada de distintas maneiras, que por vezes podem dificultar uma correta proteção à liberdade de circulação, por exemplo<sup>16</sup>. Vale lembrar que esse direito, assim como os direitos fundamentais em

---

<sup>15</sup> Se comparado com outros países, a legislação brasileira é recente. Veja-se o caso da França que, desde 1973, pela lei *Informatique et Libertés*, possui uma legislação regulamentando a Internet, posteriormente modificada para aperfeiçoamento (DONEDA, 2019, p. 191).

<sup>16</sup> Vide a questão que envolve a ADC nº. 51 e o conflito legislativo envolvendo Brasil e Estados Unidos, causando controvérsias relativas a persecução penal e as provas digitais.

geral, não se mostra absoluto, dado que podem sofrer restrições permitidas pela legislação, como, por exemplo, pela segurança pública. No entanto, assim como a legislação para o ambiente digital em geral, esse desenvolvimento ainda se mostra tímido<sup>17</sup>.

Por outro lado, há a questão sobre o direito a autodeterminação informativa, considerado direito implícito na nossa ordem constitucional, derivativo do direito à liberdade, embora também tratado como direito de personalidade (SARLET; MARINONI; MITIDIÉRO, 2017, p. 439). Trata-se de uma construção que permeia os direitos de liberdade, privacidade e também de proteção de dados pessoais e será mais adiante aprofundada. No entanto, foi referida inicialmente pelo Tribunal Constitucional Federal da Alemanha ainda em 1983, quando a Corte construiu a noção de um direito de liberdade da pessoa para decidir o que deseja informar ou não acerca de seus dados e informações (TERRA; MULHOLLAND, 2019, p. 605).

Brandt (2018, p. 80) aponta que esse direito “nada mais é do que a capacidade da pessoa determinar em princípio sobre a exibição e uso de seus dados pessoais” além de “uma intenção de firmar a liberdade do usuário de controlar as informações a seu respeito” (BRANDT, 2018, p. 79). Logo, visualiza-se se tratar de um direito relacionado à liberdade no ambiente digital, posto que é ele o maior proliferador de dados e informações da pessoa.

No âmbito legislativo, a autodeterminação informativa não é referida no Marco Civil da Internet, apesar dele garantir algumas liberdades na Internet (BRASIL, 2011). É com a Lei Geral de Proteção de Dados Pessoais que esse direito se torna fundamento para a proteção dos dados, conforme o artigo 2º, inciso II (BRASIL, 2018). Isso significa que a proteção da autodeterminação informativa, ou seja, o controle do usuário em relação aos dados e informações que pretende ou não divulgar, ampara a proteção de dados pessoais no Brasil, encontrando nela o seu fundamento.

Ressalta-se que a ideia de autodeterminação informativa se confunde com a ideia de liberdade informática, que é tratada como “um direito específico de conhecimento e controle de dados pessoais” (DONEDA, 2019, p. 170). Frosini (2003, p. 30) ressalta que se trata de um novo instituto oriundo, sobretudo, da

---

<sup>17</sup> Basta, nesse sentido, ver a morosidade em relação ao desenvolvimento da LGPD-Penal, por exemplo, que sequer projeto de lei ainda é. Trata-se de importante anteprojeto de lei para regulação dos dados pessoais para a segurança pública (ANTEPROJETO).

sociedade tecnológica, constituindo um avanço para a fronteira da liberdade humana através da sociedade. No entanto, também entende que manter as formas tradicionais de liberdade seria forçado, representando a liberdade informática como uma nova liberdade constitucional da sociedade tecnológica (FROSINI, 2003, p. 31-32).

Nesse sentido, as liberdades relacionadas à informática vêm, de alguma forma, asseguradas no ordenamento jurídico brasileiro visando ser adequadamente protegidas, mas ainda não explicitamente na Constituição. No entanto, em que medida as devassas à privacidade e dados pessoais dos usuários constituem violações à liberdade? De que forma é possível que uma adequada proteção de dados nesse novo cenário fornecer subsídios para o livre desenvolvimento da personalidade e do próprio exercício dos direitos fundamentais? Veja-se que se bem regulamentada<sup>18</sup> e com a observância os padrões e protocolos adequados, a Internet pode ser um espaço de ampliação no exercício dos direitos. Assim:

No âmbito dessa relação dupla, a internet claramente amplia as possibilidades de realização de garantias individuais. Em diversos cenários, o seu uso torna-se de certo modo, condição necessária para a realização de direitos básicos. Esse diagnóstico se faz evidente no campo da liberdade de expressão, de manifestação política e de liberdade religiosa, mas também atinge outras classes direitos fundamentais, tais como os direitos de propriedade, de livre associação, de participação política e mesmo direitos de segunda geração relacionados ao trabalho, cultura e saúde (MENDES; FERNANDES, 2020, p. 7)

No entanto, liberdade, dentro de sua importância, talvez seja um dos direitos mais afetados com as grandes operações de dados pessoais, proliferadoras de risco na Era da Informação. O alerta é realizado pelos ativistas digitais, especialmente por Julian Assange em obra coletiva a partir da excessiva vigilância:

Com o aumento da sofisticação e a redução do custo da vigilância em massa nos últimos dez anos, chegamos a um estágio no qual a

---

<sup>18</sup> A questão envolvendo a regulamentação ou a autorregulamentação constitui objeto de debate e pesquisas no ambiente acadêmico. A regulamentação por parte dos entes estatais constituiria uma maior proteção das pessoas, visando atingir o ideal do dever de proteção estatal decorrente dos direitos fundamentais (aqui, especialmente a privacidade e os dados pessoais). Por outro lado, poderia constituir uma dificuldade para a nova economia que se avizinha, daí porque, para alguns, a autorregulamentação se mostraria uma alternativa melhor. Tratam-se de dois argumentos importantes e que serão melhor aprofundados no momento oportuno. Todavia, é possível que ambos se alinhem, pois, se considerado que toda a coletividade seria destinatária dos direitos fundamentais, os grandes agentes econômicos da Internet também deveriam buscar a regulamentação das questões relativas aos dados e privacidade.

população humana dobra aproximadamente a cada 25 anos – mas a capacidade de vigilância dobra a cada 18 meses. A curva de crescimento da vigilância está dominando a curva de crescimento populacional. Não há como escapar diretamente disso. Estamos em um estágio no qual é possível comprar por apenas US\$ 10 milhões uma unidade para armazenar permanentemente os dados interceptados de um país de médio porte. Então me pergunto se não precisaríamos de uma reação equivalente. Essa é uma ameaça enorme e concreta à democracia e à liberdade de todo o planeta, e essa ameaça precisa de uma reação, como a ameaça da guerra atômica precisou de uma reação em massa, para tentar controlá-la enquanto ainda for possível (ASSANGE; *et al*, 2013, p. 55).

A afirmativa se compatibiliza com a afirmativa de Beck (2018, p. 187) de que “a percepção do risco à liberdade é o mais frágil entre os riscos globais que experimentamos até agora”, ou seja, no ambiente de uma Sociedade de Risco, posto que os danos que podem ocorrer a partir dos riscos a esse direito são irreversíveis. Além de questões de segurança pública, que permitem, em alguma medida, determinadas restrições aos direitos, muitas práticas são vetores de riscos e até mesmo violatórias à pessoa.

Decorre daí a afirmativa de Rodotà para quem, a partir da situação desse novo ambiente e a Constituição Italiana, se impõe uma “reconstrução dos direitos e liberdades referentes ao ambiente tecnológico no qual são exercidos” (RODOTÀ, 2008, p. 200). Castells (2003, p. 226) chega a definir a liberdade na Internet como um desafio nesse contexto, argumentando que:

As redes da Internet propiciam comunicação livre e global que se torna essencial para tudo. Mas a infraestrutura das redes pode ter donos, o acesso a ela pode ser controlado e seu uso pode ser influenciado, se não monopolizado, por interesses comerciais, ideológicos e políticos. À medida que a Internet se torna a infraestrutura onipresente de nossas vidas, a questão de quem possui e controla o acesso a ela dá lugar a uma batalha essencial pela liberdade.

Tanto se tornou presente nas vidas que Beck (2018, p. 190) enuncia o fenômeno da metamorfose digital, assentando o “entrelaçamento essencial do on-line e do off-line”, em alusão à influência que a Internet e a informática exercem nas vidas. No entanto, diga-se ainda que, para Castells, o modo como a Internet vem sendo conduzida é passível de gerar um verdadeiro efeito bumerangue (CASTELLS, 2003, p. 225). A afirmativa é reforçada, como visto acima, pela concepção de capitalismo de vigilância, trazida por Zuboff.

Para isso, como dito anteriormente, instrumentos protetivos dessa liberdade se mostram necessários. Como melhor exemplo, a Lei Geral de Proteção de Dados

Pessoais prevê alguns mecanismos materializadores da liberdade em sentido geral, dentre os quais é possível citar a base legal do consentimento para o tratamento de dados<sup>19</sup>. Para Danilo Doneda (2006, p. 377), a importância do instituto está na “possibilidade de autodeterminação em relação aos dados pessoais, e que esta autodeterminação deve o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento”. Trata o consentimento da expressão da liberdade da pessoa e “não deve ser tratada sob um perfil negocial e deve ter como orientação a atuação do poder de autodeterminação informativa da pessoa e da consideração dos direitos fundamentais em questão” (DONEDA, 2019, p. 329).

No entanto, até se chegar a visão sobre dados pessoais atual, a trajetória de proteção dos direitos perpassou pela proteção da privacidade, em suas mais diversas searas. Nesse sentido, a privacidade e a liberdade, tão somente, não seriam suficientes para proteger os usuários em um ambiente digital, ao que se defende o direito fundamental à proteção de dados pessoais.

Observa-se, então, que o direito à liberdade é extremamente amplo e possui diversas nuances, ainda mais em se tratando do ambiente digital. Com isso, denota-se que não somente ele é um direito amplamente passível de discussão na Era da Informação, mas, ao lado do direito à privacidade, constitui um arcabouço protetivo necessário de progressividade nesse cenário, ainda mais diante da metamorfose digital oriunda da Sociedade de Risco. Nesse sentido, a privacidade guarda relação com os direitos de liberdade, na medida em que

A privacidade passa a ser importante ou do ponto de vista comunitário, segundo o qual as pessoas precisam dela para se comunicar e pensar livremente, ou do ponto de vista econômico, segundo o qual as pessoas precisam da privacidade para interagir economicamente (ASSANGE; *et al*, 2013, p. 85-86).

Dessa forma, o próximo subcapítulo versará sobre o direito fundamental à privacidade, de modo a se verificar em que contexto surge um direito à proteção de dados pessoais e como ele se relaciona tanto com a privacidade e a liberdade nos termos aqui delineados.

---

<sup>19</sup> A base legal do consentimento se soma a outras nove bases legais para tratamento de dados pessoais previstas no artigo 7º da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), cujo rol, entende a doutrina, ser de previsão taxativa e de interpretação restritiva (MARCACINI, 2020, p. 143).

### **2.3 Privacidade, vigilância e riscos: âmbito de proteção e (in)suficiência frente a automatização das informações na Internet**

Os cenários oriundos da expansão da informática e da Internet, com o amplo uso das plataformas digitais, redes sociais, *e-commerce*, entre outros, pouco a pouco trouxe à tona maior debate sobre o direito à privacidade e meios de sua proteção diante desse ambiente. Como afirmado no primeiro capítulo, a Sociedade em Rede é um ambiente proliferador de riscos concretos, ainda mais em um cenário em que o digital cada vez mais se aproxima da realidade, diminuindo essa distância (ZUBOFF, 2020, p. 234). Aliado a isso, novos riscos são criados e há a possibilidade de novos danos ocorrerem a partir do encurtamento dessas distâncias das tecnologias em nosso cotidiano.

Como refere Bauman, diante da transformação do discurso sobre os riscos em danos colaterais, sugere-se que os efeitos positivos e negativos do advento das tecnologias de vigilância andam lado a lado, daí porque “cada aplicação consciente, honesta, de qualquer tecnologia nova abre (ao menos em princípio) uma nova área de fatalidades ainda não vivenciadas” (BAUMAN; LYON, 2013, p. 92)<sup>20</sup>.

Nesse sentido, não apenas o direito à liberdade possibilita novas interpretações, mas a própria privacidade passou por uma espécie de releitura e ampliação de um arcabouço protetivo que passou do Direito Privado ao Direito Público, inclusive de preocupação e agir estatal. Todavia, não se mostrou tal direito, sozinho, suficiente a proteger usuários no ambiente digital de riscos, carecendo de uma tutela mais ampla no tocante aos dados pessoais. O propósito aqui é analisar o percurso histórico e jurídico desse direito e de como ele sofreu essas interpretações no novo cenário, para, ao final, visualizar uma possível insuficiência protetiva que apenas com um direito à proteção de dados pessoais vem se tornando possível.

Historicamente, o direito à privacidade começou a figurar nos ordenamentos jurídicos a partir do século XIX, sendo seu contexto de formação nas legislações ligado às questões da personalidade humana e liberdade, atuando, inicialmente, como um meio de proteção da classe burguesa após as transformações da

---

<sup>20</sup> Os autores recuperam também a ideia de Beck acerca do cálculo de riscos, onde se coloca em jogo as perdas e ganhos dos riscos (BAUMAN; LYON, 2013, p. 93). Todavia, o próprio Beck admite que os riscos decorrentes da modernização, atingindo um alcance universal, talvez se mostrem imprevisíveis e até mesmo incalculáveis (BECK, 2011, p. 33), ainda mais em um cenário de estado de exceção ameaça constante, como a Sociedade de Risco (BECK, 2011, p. 28).

Revolução Industrial (RODOTÀ, 2008, p. 26). Entretanto, a ideia de intimidade e privacidade remonta a período anterior, não se evidenciando um conceito uniforme ao longo de sua história.

O direito à privacidade, a bem da verdade, jamais se apresentou como uma necessidade individual de cada ser humano, mas um verdadeiro privilégio de grupos abastados (RODOTÀ, 2008, p. 27), uma vez que se configurou como um instrumento de divisão da própria classe burguesa, não sendo “por acaso que seus instrumentos jurídicos foram predominantemente modelados com base naquele característico do direito burguês por excelência, a propriedade” (RODOTÀ, 2008, p. 27). Por outro lado, a noção de intimidade e de busca de alguma esfera mais íntima se mostra presente em algumas civilizações. Mumford, conforme Rodotà (2008, p. 26) evidencia que essa noção de intimidade surge a partir das mudanças culturais e da formação das próprias cidades, principalmente após o medievo:

a primeira mudança radical [...] destinada a modificar a forma da casa medieval foi o desenvolvimento do sentido de intimidade. Esta, com efeito, significava a possibilidade de afastar-se, por vontade própria, da vida e das atividades em comum. Intimidade durante o sono, intimidade durante as refeições, intimidade no ritual religioso e social; finalmente, intimidade no pensamento.

O autor ainda acrescenta que “o desejo de intimidade assinalou o início do novo alinhamento de classes que estava destinado a se refletir numa luta de classes sem tréguas e nas reivindicações individualistas de um período superior” (MUMFORD *apud* RODOTÀ, 2008, p. 26). Logo, percebe-se que os primórdios da proteção de privacidade e intimidade se reservou às classes abastadas da sociedade, sendo a sua ampliação resultado de conquistas sociais e da transformação das culturas e da própria civilização. Em seus primórdios, figurava-se muito mais como um direito em sentido negativo, de afastamento, tendo em vista que “o direito a abordou durante muito tempo foi pela sua associação à busca de alguma forma de isolamento, refúgio ou segredo” (DONEDA, 2019, p. 29).

Nesse sentido, uma das primeiras teorizações jurídicas sobre o direito à privacidade é conferido pelo artigo *The right to privacy*, de autoria de Louis Brandeis e Samuel D. Warren em 1890, que justamente reforça a ideia da privacidade como um ideal de isolamento (BRANDEIS; WARREN, 1890). Nela, os autores aduzem a preocupação de que “o maldizer não era mais o recurso do ocioso e dos perversos,

*mas tinha-se tornado um negócio, perseguido com indústria e audácia”* (RUARO; RODRIGUES, FINGER, 2011, p. 51) (grifo do autor). É a partir disso que o célebre artigo traz a ideia de direito à privacidade como um verdadeiro direito de ser deixado só (DONEDA, 2019, p. 30),

Logo, a ideia de privacidade guardaria relação com uma distinção entre aquilo que seria público, ou seja, disponível para as pessoas em geral, e alguma esfera mais íntima do indivíduo, não disponível a todos. Nesse contexto é que surge, por exemplo, a teoria alemã das esferas que

utiliza um esquema de esferas concêntricas para representar os diferentes graus de manifestação do sentimento de privacidade: a esfera da intimidade ou do segredo (Intimsphäre); a esfera privada (Privatsphäre) e, em torno delas, a esfera pessoal, que abrangeria a vida pública (Öffentlichkeit). Tal teoria, que hoje chega a ser referida pela própria doutrina alemã como a teoria da ‘pessoa como uma cebola passiva’, foi desenvolvida e posteriormente perdeu a sua centralidade nesta matéria (DONEDA, 2008).

Trata-se, contudo, de visão já superada, pois a compreensão atual da privacidade compreende diversos outros fatores, sendo um dos mais importantes as questões relativas às redes sociais, Internet e a influência dos dados pessoais. Além disso, a teoria das esferas demonstra uma visão muito engessada de um direito que se encontra em constante mutação. Nesse sentido, Farinho (2006, p. 45) afirma a “[...] dificuldade em reconduzir conteúdos a cada uma das esferas, existe a possibilidade de, pela sua fluidez, os conteúdos migrarem de uma esfera para outra”, o que dificultaria uma certa categorização da privacidade.

Bolesina e Gervasoni (2020, p. 3), por sua vez, trazem a diferenciação entre privacidade enquanto bem existencial, típico do comportamento humano, e o direito à privacidade, destinado à proteção desse bem. Acrescentam que ele é

algo vinculado majoritariamente à modernidade jurídica, amarrado, sobretudo, nos debates sobre a distinção dos espaços públicos e privados. Ao menos no ocidente, o direito a privacidade aparece muito claramente na modernidade jurídica, (1) reforçando a ideia de uma dicotomia público-privado, (2) tornando a privacidade em si um privilégio de classe e (3) formatando um imaginário interiorista (BOLESINA; GERVASONI, 2020, p. 3).

Com isso, após a superação da ideia de direito de ser deixado só, ou seja, uma formatação interiorista da privacidade, com o surgimento do Estado de Bem-Estar Social, “a transformação sentida é uma ampliação do modelo individualista,

patrimonial e solitário (interiorista) para um modelo social de privacidade” (BOLESINA; GERVASONI, 2020, p. 8).

Rodotà, por outro lado, trata sobre uma diferente visão da privacidade, com mudanças ocasionadas a partir do surgimento da Internet e da questão dos dados pessoais. O autor entende a existência de quatro novas tendências sobre o conceito de privacidade, quais sejam:

1. do direito de ser deixado só ao direito de manter o controle sobre as informações que me digam respeito;
2. da privacidade ao direito à autodeterminação informativa;
3. da privacidade à não-discriminação;
4. do sigilo ao controle (RODOTÀ, 2008, p. 97-98).

Logo, a visão concernente à privacidade no ambiente informacional traça novos contornos que possuem relação com a proteção de dados pessoais e autodeterminação informativa. Bolesina e Gervasoni (2020, p. 10) trazem que “a privacidade dá franca atenção aos elementos informacionais inerentes ao ‘pessoal’, podendo eles serem sigilosos/secretos ou não, mas sempre pessoais”. Assim, conforme os autores, a “sequência lógica de tutela clássica consubstanciada na ordem ‘pessoa-informação-sigilo’ passa a ser ‘pessoa-informação-circulação-controle’” (BOLESINA; GERVASONI, 2020, p. 2020).

Mais recentemente, a privacidade constitui preocupação com o debate envolvendo a Internet e os grandes bancos de dados e informações. Nesse contexto, uma das contribuições sobre uma sistematização do direito à privacidade é a sua taxonomia. Atribui-se a Daniel Solove a ideia de uma taxonomia da privacidade, na tentativa de conceituar e analisar as questões relacionadas a esse direito.

Segundo essa taxonomia, é possível dividi-la em quatro grupos que tratam de atividades danosas à privacidade: coleta de informação, materializada através da vigilância e interrogação em busca da informação; processamento de informação, que pode se dar através da agregação, identificação uso secundário, exclusão ou insegurança em relação a informação; disseminação, que pode ocorrer por diversas maneiras, dentre elas a distorção, apropriação, quebra de confidencialidade, entre outros; invasão, que se materializa pela intrusão ou interferência decisional (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 51-52). Como se observa, a taxonomia proposta trabalha já com a ideia das tecnologias da informação e possui relação

com a proteção de dados pessoais, que, para alguns, está abrangida pela proteção da privacidade.

Dessa maneira, é notório que essa nova forma de se entender a privacidade guarda intrínseca relação com dados pessoais, autodeterminação informativa e a própria liberdade. Instrumentos protetivos, como antes trabalhado, muitas vezes buscam materializar a defesa a cada um desses direitos, que são reconhecidos na nossa Constituição.

No campo do caráter fundamental desse direito, é preciso destacar que a privacidade assumiu especial relevância na Constituição da República de 1988. Nesse sentido:

No Brasil, assim como em outros diversos Estados, o direito à privacidade é assegurado constitucionalmente como direito humano fundamental. A Constituição Federal brasileira não se restringe apenas ao direito à privacidade, apresentando abrangência em relação à preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações [...] (FORTES; BOFF, 2014, p. 119).

Na Constituição brasileira o direito à privacidade se encontra positivado no rol de direitos fundamentais do artigo 5º, especialmente nos incisos X, XII e XIII. Apesar de não haver referência expressa à privacidade, a privacidade se materializa na proteção da intimidade, vida privada, inviolabilidade do domicílio e das comunicações (BRASIL, 1988), o que evidencia também a sua amplitude no nosso ordenamento jurídico. Do mesmo modo, encontra-se prevista a inviolabilidade da vida privada no artigo 21 do Código Civil (BRASIL, 2002).

No âmbito da proteção internacional e de direitos humanos, a privacidade também encontra respaldo jurídico. Na Declaração Universal dos Direitos Humanos, a proteção à vida privada está positivada no artigo 12, na medida em que garante a não interferência à vida privada das pessoas (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948). Por sua vez, no âmbito do continente americano, tal direito também encontra resguardo na Convenção Americana sobre Direitos Humanos, da qual o Brasil é signatário, na medida em que seu item 2 do artigo 11, é protegida a vida privada contra as ingerências arbitrárias (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969).

Por sua vez, no continente europeu, a preocupação sobre a proteção à privacidade também se faz muito presente. Afora as questões relativas à proteção

dos dados pessoais, que será trabalhada no terceiro capítulo, a privacidade tem sido preocupação constante na Europa, aliada, certamente, a essa proteção dos dados pessoais. No entanto, a ideia de privacidade se visualiza um pouco diferente da ideia de proteção de dados pessoais, pois, conforme a Carta de Direitos Fundamentais da União Europeia, em seu artigo 7º, o direito à vida privada é protegido de forma apartada à proteção dos dados pessoais, que encontra seu fundamento no artigo 8º (UNIÃO EUROPEIA, 2000). Vale destacar que a proteção à vida privada abrange a proteção domiciliar e da própria comunicação privada. Do mesmo modo, o direito à privacidade está resguardado no artigo 8º da Convenção Europeia dos Direitos do Homem (UNIÃO EUROPEIA, 1950).

Dessa forma, visualiza-se que a privacidade é de há muito resguardada pelos documentos internacionais, não apenas nas Cartas Constitucionais garantidoras de direitos fundamentais. No entanto, é possível perceber que a América Latina não dispõe, atualmente, de instrumentos de proteção comunitária como dispõe a União Europeia. Fato é que os instrumentos de proteção são diversos e se encontram em constante aperfeiçoamento, sobretudo diante do desenvolvimento tecnológico.

Observa-se que “dos direitos fundamentais que dizem respeito à proteção da dignidade e personalidade humanas, o direito à privacidade (ou vida privada) é um dos mais relevantes” (SARLET; MARINONI; MITIDIERO, 2017, p. 445). Na atual ordem constitucional, ele opera em uma dimensão subjetiva e outra objetiva: na primeira, age como um direito de defesa, na qual impede a interferência de outros na sua esfera privada e de que a pessoa possa livremente decidir sobre sua vida pessoal. Vale lembrar que essa dimensão dos direitos fundamentais “corresponde à característica desses direitos de conferir ao seu titular a pretensão de exigir de alguém – do Estado e dos demais particulares – um determinado comportamento em seu favor” (VIEIRA, 2007, p. 69).

Por sua vez, a existência desse direito faz também que ele opere na dimensão objetiva, se demonstra em um dever do Estado de conferir proteção e garantia da vida privada (SARLET; MARINONI; MITIDIERO, 2017, p. 449). Como já demonstrado, a dimensão objetiva se materializa também na criação da Lei Geral de Proteção de Dados, por exemplo, pois, apesar de visar em específico os dados pessoais, garante instrumentos de proteção à privacidade, dado que direitos correlatos, bem como enuncia a criação de uma Política Nacional de Proteção de

Dados Pessoais e Privacidade (BRASIL, 2018). Além disso, é importante destacar que a dimensão objetiva evidencia uma eficácia horizontal desse direito, como antes referido, que deve ser observado também pela coletividade, incluindo os particulares<sup>21</sup>. Decorre disso a conclusão de Vieira (2007, p. 110), a partir de estudo jurisprudencial, que

[...] no ordenamento jurídico nacional, apesar de inexistir exposto dispositivo constitucional determinando a *aplicação direta ou imediata dos direitos fundamentais nas relações entre particulares*, tal medida configura-se como uma decorrência lógica do caráter objetivo dos direitos fundamentais. *Enquanto garantia integrante do estatuto axiológico do ordenamento jurídico nacional, o direito à privacidade estende-se por todos os ramos do direito, vinculando tanto o poder tanto o poder público como os demais particulares de forma direta ou imediata [...]* (grifo do autor).

Vale destacar que existem algumas divergências acerca do conceito sobre o que seria o direito à privacidade, eis que autores referem vida privada, intimidade e privacidade por vezes como sinônimos, por vezes como direitos distintos (DONEDA, 2019, p. 104-105), demonstrando a elasticidade do conceito, como as suscitadas anteriormente. Doneda afirma que o fato do conceito não possuir uma definição unânime e definitiva não deve ser vista como um defeito, mas, na verdade, como uma própria característica imanente a tal direito, pelo fato de que, historicamente, passou por diversas mudanças em sua compreensão (DONEDA, 2019, p. 101-102). A mesma advertência é feita por Vieira (2007, p. 134-135) com o seguinte raciocínio:

Aspecto que ainda merece atenção quanto à amplitude do âmbito de proteção do direito à privacidade diz respeito à constatação do caráter eminentemente elástico e variável dessa garantia. O tempo, o espaço e o titular podem atuar como elementos determinantes em relação ao grau de abrangência dessa garantia. Quanto ao tempo, verifica-se que em décadas passadas a proteção de dados pessoais não se destacava tão relevante diante da inexistência de recursos tecnológicos aptos à interconexão dessas informações. Quanto ao espaço, observa-se que certas condutas, perniciosas à privacidade em determinadas comunidades, em outras recebem tratamento sem reações adversas, o que leva à constatação de que tal garantia é passível de flexibilização conforme evidenciem adequação ou não aos costumes adotados pelos grupos sociais. A proteção do isolamento pessoal, lembre-se, não é resguardada em comunidades indígenas (VIEIRA, 2007, p. 134-135).

---

<sup>21</sup> Importante fazer a ressalva de que essa noção de eficácia horizontal não é um dado adquirido a nível mundial, uma vez que encontra críticas com Dimoulis e Martins (2018), além do fato de não ser unânime nos países da Europa. Aqui, é preciso conferir a devida importância, especialmente diante do tamanho que as plataformas digitais assume no campo do tratamento de dados.

Nesse sentido, o seu âmbito de proteção, apesar de ser delimitado, possui ampla margem de interpretação<sup>22</sup>, que, por muitas vezes, se assemelha à intimidade, por exemplo. Sarlet aponta que vida privada, intimidade e privacidade devem ter uma análise conjunta, haja vista a impossibilidade de serem dissociados, apesar de vida privada se referir a algo mais restrito, dividindo as esferas de proteção em esfera íntima, esfera privada e esfera social (SARLET: MARINONI, MITIDIERO, 2017, p. 446). O mesmo raciocínio é aplicável quando se trata da relação com o direito à proteção de dados pessoais.

Entretanto, com a ascensão da internet, o direito à privacidade passou por nuances que foram conferindo a ele maior atenção por parte dos ordenamentos e também uma expansão de seu conceito. Com a ascensão da rede, destaca-se que a ameaça à privacidade “é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que desvendam a vida dos indivíduos, sem sua autorização e até sem seu conhecimento” (SILVA, 2017, p. 211-212).

A questão ganha outros contornos quando se visualiza a privacidade no seio de riscos e perigos oriundos da Internet e desse desenvolvimento tecnológico. Como pontua Leal (2020, p. 366):

Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infindáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos.

Em tais cenários, as mutações ocorrem inclusive sobre os objetos de tutela jurídica envolvendo o direito à privacidade e intimidade, pois, da tradicional liberdade negativa (livre de ingerência externa), passa a ser integrado como bem tutelado o direito de autodeterminação informativa relacionada ao indivíduo e sujeito de direito. Ou seja, passa-se a reconhecer a todo o cidadão a faculdade de escolher o que deseja fazer com os seus dados pessoais – e o que não deseja também.

---

<sup>22</sup> A partir disso, visualizado dentro das casuísticas, a solução diante de colisão envolvendo outros direitos fundamentais e a privacidade deve ser objeto de interpretação dos direitos fundamentais, utilizando-se, por exemplo, o próprio teste de proporcionalidade, o que não é objeto do presente estudo. Todavia, como é o caso da privacidade das pessoas notoriamente públicas e conflito liberdade de informar e de expressão, Vieira (2007, p. 136) ainda lembra que “embora seja mais restrito o âmbito de proteção do direito à privacidade das pessoas públicas e notórias, mesmo em relação a tais pessoas deve ser preservada uma parcela de confidencialidade necessária ao desenvolvimento de sua personalidade e à manutenção de sua paz interior”. Logo, trata-se de direito fundamental a ser analisado e interpretado com cautela frente as colisões.

Um dos cenários de maior risco à privacidade é a emergência e os Estados de Exceção, fundados, por exemplo, nas questões de segurança pública e de emergência sanitária, operadoras de restrições a esse direito fundamental. Leal (2020, p. 361) traz o exemplo do Estado de Urgência promovido na França a partir de ataques em Paris, no ano de 2015, sob o fundamento da segurança pública e nacional, onde restou autorizada a promoção acesso a domicílios sem autorização judicial, devassando-se a privacidade do morador em nome de tais direitos.

Igualmente, a questão envolvendo a crise sanitária da pandemia de Covid-19 também legou situações envolvendo esse direito. A fim de obter o controle sobre as taxas de contaminação e alastramento da pandemia, inúmeras formas de restrição à privacidade foram tomadas no contexto da emergência e dos riscos que se seguiram, a exemplo do monitoramento de celulares para fins de controle de aglomerações<sup>23</sup> (LEAL, 2020, p. 368). Trata-se de restrições que, obedecendo-se ao princípio da legalidade, devem ser fundamentadas e motivadas por meio de lei. Nesse ponto, Leal (2020, p. 368) aduz que

Por certo que aqui já temos outros desafios que é o de densificar materialmente – e no caso concreto – os níveis e possibilidades das *medidas proporcionais e estritamente necessárias* ao escopo da norma e diante de cenários os mais particulares existentes – como o da segurança da saúde pública na pandemia.

E isto se torna necessário quando vemos que, na China, ponto inicial da pandemia provocada pelo corona vírus, foram e são utilizados, até agora, *drones*, tecnologia de reconhecimento facial, *scanners* infravermelhos, além da implementação de aplicativo para classificar as pessoas de acordo com o risco de contágio, sendo tal informação transmitida às autoridades competentes.

Para Moura e Ferraz (2020, p. 5) o caminho perseguido para a pandemia é a imprescindibilidade de que se sigam os princípios e padrões de proteção de dados. Ainda, acrescentam que haveria duras consequências "para a humanidade a adoção de tecnologias intrusivas por natureza ou a adaptação de serviços que não foram criados com a finalidade de entender o comportamento das pessoas respeitando a sua privacidade" (MOURA; FERRAZ, 2020, p. 5).

No Brasil, objeto de grande discussão perante o Supremo Tribunal Federal,

---

<sup>23</sup> O autor ainda traz que "o problema é que mecanismos de gestão de crises imprevisíveis como a do corona vírus, para as quais inexistem protocolos fechados e testados de tratamento e evitação, levam o Estado de direito a desenvolver políticas de enfrentamento muitas vezes invasivas daqueles direitos individuais referidos, como é o caso do chamado sistema de controle inteligente para evitar aglomerações, utilizando o monitoramento indiscriminado de celulares das pessoas" (LEAL, 2020, p. 358).

justamente no seio dos riscos e danos causados pela pandemia, foi o ajuizamento das Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6390 e 6393, que impugnaram a Medida Provisória nº. 954/2020<sup>24</sup> (BRASIL, 2020) perante a Corte. A ação pautou diversas questões relativas à medida, que se destinava a produção de estatística no contexto da pandemia, a partir de, nomeadamente, dois direitos fundamentais: a privacidade e a proteção dos dados pessoais. No âmbito dos dados pessoais, trata-se de decisão histórica para o Brasil e será oportunamente trabalhada.

A Medida Provisória impunha o dever de compartilhamento de dados e informações das operadoras de telefonia com a Fundação IBGE no âmbito da crise sanitária, de modo a devassar a privacidade das pessoas, na tentativa de produção de estatística oficial (BRASIL, 2020). A medida foi suspensa pela Corte, tendo em vista a absoluta desproporcionalidade da medida e carência de fundamentação, ainda mais na vigência da Lei Geral de Proteção de Dados Pessoais. Por meio de cinco artigos, a legislação possibilitava uma espécie de coleta de dados pessoais durante a situação de crise sanitária sem parâmetros mínimos.

A questão é bem demonstrada pelo voto do Ministro Luis Roberto Barroso quando aduz que “a dualidade que se coloca, aqui, nesta ação é precisamente essa: uma tensão entre a importância dos dados no mundo contemporâneo e os riscos para a privacidade que a sua malversação representa para todos nós” (BRASIL, 2020, p. 48). É preciso destacar que a própria Lei Geral de Proteção de Dados Pessoais possibilita a operação de dados pessoais em razão da execução de políticas públicas (BRASIL, 2018). No entanto, como bem argumentou o Ministro Barroso:

Portanto, eu concluo o meu voto, Presidente, com a seguinte síntese: Compartilhamento de dados pessoais para fins de produção de estatísticas somente será compatível com o direito à privacidade se: 1) a finalidade da pesquisa for precisamente delimitada; 2) o acesso for permitido na extensão mínima necessária para a realização dos seus objetivos; 3) forem adotados procedimentos de segurança suficientes para prevenir riscos de acesso desautorizado, vazamentos acidentais ou utilização indevida (BRASIL, 2020, p. 46).

---

<sup>24</sup> Conforme consta na medida, ela “dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (**COVID-19**), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.” (BRASIL, 2020).

Lima (2020, p. 89) acrescenta que “compete ao Estado, enquanto detentor das informações individuais pertinentes à pessoa, tomar atitudes concretas tendentes a efetivar a proteção da privacidade, tanto no que diz aos cadastros em meio físico, quanto em meio digital”<sup>25</sup>, materializando o seu dever de proteção estatal. A autora ainda acrescenta, nessa toada, que “esses aspectos colocam na ordem do dia a imperiosa tarefa da doutrina de destacar os desafios da tutela dos direitos de personalidade hodiernamente” (LIMA, 2020, p. 89).

Percebe-se que a discussão enfrentada trouxe ainda mais à tona a importância dos dados pessoais para as ações governamentais, mas também a necessidade de uma proteção da privacidade em conjunto com a dos dados pessoais. Nesse sentido, evidencia que o direito à privacidade, por si só, não dá conta de um âmbito de proteção de modo a garantir a defesa do particular contra as ingerências estatais e privadas.

Assim, caracterizam-se novos riscos que “escapam inteiramente à capacidade perceptiva humana imediata. Cada vez mais estão no centro das atenções ameaças que com frequência não são nem visíveis nem perceptíveis para os afetados” (BECK, 2011, p. 32). A dificuldade de se perceber ameaças à privacidade<sup>26</sup> evidencia a dificuldade de se proteger os direitos na Sociedade de Risco.

Sobretudo, com as ingerências das grandes empresas de tecnologia, os riscos à privacidade se elevaram. No entanto, a vigilância estatal também se faz cada vez mais presente. Lima (2020, p. 66) ressalta que:

Sempre que se fala em *Big Data*, pensa-se nas grandes empresas que coletam informações na Internet (*Google, Facebook* e etc.), mas não se pode olvidar que o Estado é o precursor nesta atividade, isto é, de coletar informações pessoais e as armazenar.

Os riscos são muitos e há pouco tempo o mundo tomou conhecimento de atividades de espionagem da *U.S National Security Agency (NSA)*, que interceptou e armazenou 1,7 bilhões de e-mails e ligações de cidadão norte-americanos e de outras nacionalidades, inclusive autoridades (grifo do autor).

<sup>25</sup> Para além da discussão sobre a proteção de dados pessoais, para a necessidade de se falar na proteção às pegadas digitais, que se ampliam à mera proteção de dados, havendo necessidade de construção de regulações e instrumentos protetivos.

<sup>26</sup> A afirmativa de Beck evidencia um problema rotineiramente visualizado na privacidade diante do ambiente digital. Muitas vezes, a privacidade de um usuário é devassada sem ao menos que ele tenha a consciência dessas ameaças e riscos, percebendo tão somente quando os danos já aconteceram. É o caso, por exemplo, dos grandes vazamentos e espionagens envolvendo agentes de Estado, denunciados pelos ativistas do *site Wikileaks*, cujos riscos e consequentes danos foram conhecidos quando o escândalo veio a público.

Conclui-se que a questão sobre a necessidade de uma proteção de dados pessoais, de caráter estrito, se mostra necessária diante da Sociedade de Risco. Denota-se que as transformações econômicas e sociais oriundas da Sociedade em Rede acarretaram transformações jurídicas mediante o aprimoramento e criação de novos direitos, que extrapolam a proteção da liberdade e da privacidade. Esses novos delineamentos da privacidade na Era da Informação, fizeram com que surgisse essa nova disciplina jurídica autônoma da proteção da privacidade, erigindo a proteção de dados pessoais, cujo direito fundamental amplia a esfera de proteção pessoal.

Nesse sentido, verifica-se que “a proteção de dados pessoais, em suma, propõe o tema da privacidade, porém, modifica seus elementos; aprofunda seus postulados e toca nos postulados centrais dos interesses em questão” (DONEDA; 2019, p. 173). Conforme lição de Rodotà, “[...] a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas” (RODOTÀ, 2008, p. 17).

Além disso, a observação que Doneda (2020, p. 327) é extremamente pertinente nesse contexto, quando se busca delimitar privacidade e proteção de dados pessoais:

O direito à privacidade atualmente apresenta seu caráter individualista e exclusivista diluídos, e assume feições de uma disciplina na qual merecem consideração a liberdade e o livre desenvolvimento. Nesse panorama, a proteção de dados pessoais assume o caráter de um direito fundamental.

[...] A privacidade e a proteção de dados pessoais relacionam-se diretamente com múltiplos valores e interesses, não raro contraditórios entre si. Alertas sobre a ‘morte da privacidade’ ou considerações sobre ‘por que a privacidade é importante’, por mais autorizados e pertinentes que sejam, são enfoques unidimensionais do problema. A proteção de dados pessoais deve definir, mais que tudo, a quem cabe o controle sobre os dados pessoais – e assim, consequentemente, realizar uma forma de distribuição de poder na sociedade.

Dessa maneira, fala-se de um direito fundamental à proteção de dados pessoais, cuja proteção possui um campo específico e próprio. No ambiente digital, a análise dos direitos fundamentais nessa seara deve ser feita de modo multifacetado, daí porque se visualizar o contexto como Sociedade de Risco e a referência de Beck (2018, p. 189) a metamorfose digital e um poder central digital

autônomo. Imperioso referir que privacidade e proteção de dados, apesar de direitos diferentes, também se complementam, o que não impede uma análise que entrelace tais direitos. O aprofundamento sobre a temática será realizado no capítulo seguinte, onde se analisará o direito fundamental à proteção de dados pessoais, suas pertinências e o modo como uma legislação protetiva influi na proteção da liberdade no ambiente digital.

### **3 O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: POSSIBILIDADES À LIBERDADE NA ERA DA INFORMAÇÃO**

A partir do exposto nos capítulos anteriores foi possível observar de que maneira determinados direitos fundamentais foram afetados com o surgimento da Internet e da operação com dados pessoais. A tese proposta anteriormente é de que a estruturação da Sociedade em Rede, com a globalização e ampliação da Internet, possibilita ser ela visualizada também como uma Sociedade de Risco, nos termos propostos por Beck. Esse fenômeno das mudanças permitidas pela Internet foi tratado por Ulrich Beck como a metamorfose digital, não se restringindo a meras modificações no estrato social, mas de complexas nuances em escala global, tendo como substrato central a proteção de dados pessoais (BECK, 2018, p. 190).

Então, os direitos fundamentais, em um ambiente digital que é descentralizado e desterritorializado, também sofrem influência nos cenários de riscos. Nesse sentido, como visto, dois foram os direitos abordados com maior profundidade: a liberdade e a privacidade. Assim, foi possível perceber a mudança ocorrida em tais direitos e como a privacidade do modo como se compreende atualmente não se mostra, por si só, suficiente a proteger o titular de seus direitos.

Com as premissas anteriormente assentadas, o presente capítulo tem o condão de analisar como a proteção jurídica dos dados pessoais possibilita um adequado exercício dos direitos fundamentais, nomeadamente a liberdade, no seio da Sociedade de Risco.

Para tanto, busca-se inicialmente verificar a existência, fundamentação e progressão histórica do direito fundamental à proteção dos dados pessoais que, no Brasil, é tido como um novo direito fundamental, inserido no rol do artigo 5º da Constituição. Logo após, será abordado com maior profundidade o conjunto legislativo que envolve a proteção de dados pessoais, com especial destaque a formas de tratamento, bases legais e instrumentos possíveis para a proteção desse novel direito. A partir disso, visualiza-se que as premissas possíveis para a análise proposta da pesquisa se encontram postas, onde se analisará com especificidade o modo como essa proteção e os dispositivos legais permitem uma tutela da liberdade no ambiente digital.

### 3.1 Fundamentos para o direito fundamental à proteção de dados pessoais

O direito sobre a proteção dos dados pessoais<sup>27</sup> não é tema discutido há muito tempo no Brasil, de modo que as normas que disciplinam o tratamento de dados pessoais, principalmente na Internet, são recentes. É possível, com isso, referir sobre a existência de um sistema de proteção dos dados pessoais no ordenamento jurídico, cujo centro se encontra o seu direito fundamental, que somente foi consagrado de modo expresso na Constituição no ano de 2022, inserindo-o no rol do artigo 5º a disciplina da proteção de dados pessoais em caráter fundamental (BRASIL, 1988).

A concepção de que o direito à proteção de dados pessoais é fundamental e que não se engloba no conceito de direito à privacidade é construção teórica recente, que se iniciou, sobretudo, a partir do desenvolvimento das tecnologias da informação, de modo que a mera concepção da privacidade, seja como direito a estar só ou como direito ao controle dos dados e informações, não se mostrava suficiente, erigindo a disciplina própria aqui estudada. Tal foi o entendimento do Supremo Tribunal Federal por ocasião do julgamento da ADI 6387, quando a Corte, pela primeira vez, se pronunciou sobre o caráter fundamental desse direito, em julgamento que tratava sobre a tese da inconstitucionalidade da Medida Provisória 954/2020, eis que violava o sigilo e proteção dos dados.

A referida medida dizia respeito à obrigatoriedade de compartilhamento dos dados telefônicos das operadoras ao IBGE durante a pandemia de COVID-19 (BRASIL, 2020, p. 02). Em seu voto, afirmou o Ministro Gilmar Mendes que o direito fundamental à proteção de dados pessoais “não mais se adstringe à demarcação de um espaço privado, mas, antes, afirma-se no direito à governança, transparência e sindicabilidade do tratamento de dados compreendidos em acepção abrangente” (BRASIL, 2020, p. 20). No mesmo sentido, declarou:

A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero

---

<sup>27</sup> Tratando-se de capítulo que se debruçará mais firmemente sobre a temática, importa conceituar dados pessoais. Consoante a lição de Sarlet e Caldeira (2019, p. 2), “dados pessoais são todas as informações de caráter personalíssimo caracterizadas pela identificabilidade e pela determinabilidade do seu titular”. Tal conceito é ainda ampliado quando se fala em dados pessoais sensíveis, que são “aqueles que tratam sobre a origem racial e étnica, as convicções políticas, ideológicas, religiosas, as preferências sexuais, os dados sobre a saúde, os dados genéticos e os biométricos” (SARLET; CALDEIRA, 2019, p. 2).

encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas.

Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade (BRASIL, 2020, p. 21).

O julgamento em questão é histórico e paradigmático na compreensão do que é o direito fundamental à proteção de dados, considerando que foi a primeira vez que o Poder Judiciário se manifestou sobre ele, conferindo-lhe tamanha importância, mesmo que, à época, ainda não estava positivado na Constituição.

De outro lado, diversos outros países já reconheciam o caráter jusfundamental da proteção de dados pessoais em suas Constituições. Trata-se de um movimento internacional que, reconhecendo a importância jurídica dos dados pessoais e os riscos possíveis à liberdade humana, busca proteger os cidadãos no ambiente digital.

De fato, uma das experiências mais sólidas e reconhecidas em todos os seus contornos é a da Itália. Muito bem desenvolvido pelo jurista italiano Stefano Rodotà, o sistema de proteção criado pela Itália em muito inspirou o brasileiro (LIMA, 2020, p. 169). Semelhantemente ao Brasil, a legislação italiana disciplina o tratamento dos dados pessoais a partir da noção de dignidade humana, que é muito cara ao direito brasileiro (LIMA, 2020, p. 175). Nesse sentido, o sistema italiano<sup>28</sup> em muito observa os ditames do continente europeu e o modo como a Europa trata sobre a proteção de dados, sobretudo a partir da criação do GDPR.

Com isso, o pano de fundo de todo o ordenamento é considerar o direito à proteção de dados pessoais como um direito fundamental, que está previsto na Carta de Direitos Fundamentais da União Europeia, em seu artigo 8º. Inclusive, Rodotà defende que tal direito deve ser visto em um contexto ainda mais amplo que previsto na Carta de Direitos Fundamentais, sobretudo em razão dos direitos que surgem a partir do desenvolvimento das tecnologias (RODOTÀ, 2008, p. 17).

Sem pretender traçar um estudo de direito comparado ou adentrar nos regramentos próprios no âmbito internacional, denota-se que as experiências estrangeiras em muito acrescentam para a possibilidade de se tracejar uma proteção em unidade a nível global, principalmente pelo caráter global da Internet. As relações

---

<sup>28</sup> Outro país a conferir destaque à proteção de dados pessoais é Portugal, que, no artigo 35 de sua Constituição, garante-a como direito fundamental e segurança contra terceiros e uso indevido.

entre a LGPD e o GDPR, que serão oportunamente estudadas, evidenciam essa possibilidade e necessidade. Todavia, importante destacar a lição de Silveira e Froufe sobre a realidade da União Europeia e de seu sistema de proteção quando afirmam que

RGPD concretiza a solução adotada pela CDFUE quando autonomizou o direito à proteção de dados pessoais (art. 8.º) relativamente ao direito à proteção da vida privada (art. 7.º). Para o direito da União Europeia nem todos os dados pessoais são suscetíveis, pela sua natureza, de causar prejuízo à privacidade da pessoa em causa – mas devem ser igualmente protegidos. (SILVEIRA; FROUFE, 2018, p. 20).

Para tais autores, a relação entre a questão jurídica e “a proteção de dados pessoais converteu-se na questão jusfundamental identitária dos nossos tempos para que o projeto do humanismo não se torne irrelevante” (SILVEIRA; FROUFE, 2018, p. 7). Trata-se daquilo que Beck (2018, p. 190) afirmou como expectativa e efeito colateral do risco global, qual seja a necessidade de um “humanismo digital”, pautado nos ideais da liberdade e da proteção de dados pessoais.

Por trás de toda a perspectiva desse direito, reside uma grande complexidade que permeia diversos outros direitos fundamentais já consagrados, de forma que a proteção aos dados pessoais não se mostra, diante da Era da Informação e da Sociedade de Riscos, um direito desatento aos demais direitos fundamentais. Nessa seara, as implicações da proteção de dados alcançam, ao fim e ao cabo, os limites e proteção da própria liberdade no espaço digital.

Albers (2016, p. 29-30), quando trata da complexidade da proteção de dados pessoais, aduz que a disciplina da proteção de dados não busca proteger tão somente os dados, mas às pessoas aos quais aqueles dados se referem, não sendo uma concepção isolada apenas dos dados, de caráter individualista, distanciando-se de uma ideia patrimonialista dos dados pessoais.

Trata-se, então, para a jurista alemã, de uma necessidade de “compreensão multidimensional de direitos fundamentais; e, em decorrência disso, a proteção de dados inclui um conjunto de direitos que precisam ser descritos de uma maneira nova” (ALBERS, 2016, p. 33), de forma que as pessoas possam ter conhecimento dos dados, obter a informação, participar e influenciar nas questões relativas aos dados pessoais (ALBERS, 2016, p. 34). Aqui, inclusive, é possível se falar, por exemplo, sobre um aspecto democrático na gestão estatal dos dados pessoais,

matéria que não é comportada pelo presente estudo.

Portanto, o direito relativo aos dados se trata de um instrumental vasto a se relacionar com outros direitos, apto a atender “um conjunto complexo de interesses dignos de tutela” (ALBERS, 2016 p. 38), cuja compreensão deve ser “multidimensional de direitos fundamentais e exige descrições inteiramente novas dos interesses protegidos” (ALBERS, 2016, p. 38).

Essa perspectiva de se encarar o direito fundamental em questão é uma virada de chave em uma economia informacional, onde o dado pessoal, em verdade, é visto como uma mercadoria. Daí a afirmativa de Rodotà de que “o direito à proteção de dados tem a ver com a proteção da personalidade, não da propriedade” (RODOTÀ, 2008, p. 19).

Aliás, é essa a concepção que faz com que se busque descolar a visão de dados pessoais como algo estático em razão da existência das complexidades que lhe são inatas. Autores defendem, inclusive, que o direito fundamental à proteção de dados é direito indisponível, cuja perspectiva faz descolar da ideia de dados pessoais como propriedade, ainda mais diante dos meios virtuais e da forma econômica que os dados vêm assumindo.

Sombra (2019, p. 68) traça um interessante panorama entre o direito à proteção de dados pessoais e o consentimento, uma vez que este é um elemento essencial desse direito e da possibilidade de dispor sobre sua privacidade ou seus dados. Todavia, o autor torna ele distante da ideia de proteção enquanto personalidade:

No entanto, a cada dia o consentimento tem se tornado mais insuficiente ou tem sido fornecido em condições de desigualdade ou em circunstâncias alheias às manifestações de poder. Por essa razão, o consentimento tem deixado de ser a peça chave do controle sobre os dados pessoais e aberto espaço para outras ferramentas como a *accountability*. A rigor, quanto maior a percepção da ideia de propriedade vinculada aos dados pessoais, maior será o enfoque no consentimento. Por outro lado, quanto maior a percepção de que a privacidade e proteção de dados envolve um direito fundamental indisponível, menor o papel do consentimento (SOMBRA, 2019, p. 68) [grifo do autor].

Logo, observa-se que o autor entende que haveria uma margem de indisponibilidade desse direito quando descolada da ideia de consentimento. Essa percepção mitiga, de certa forma, a figura da base legal do consentimento, ampliando a esfera de tutela do direito não apenas a partir dessa base, mas do direito por si pró-

prio. Ou seja, quando se ampliam os instrumentos de disponibilidade do direito, distancia-se da ampla proteção a ele<sup>29</sup>.

No âmbito do ordenamento constitucional pátrio, a tramitação a PEC 17/2019 junto ao Poder Legislativo Brasileiro, constituiu importante virada de chave na seara dos direitos fundamentais diante das novas tecnologias, pois buscou acrescentar “o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria” (BRASIL, 2019). Em parecer da Comissão de Constituição e Justiça, houve alterações no texto inicial, ao que se propôs uma nova redação ao artigo XII do artigo 5º da Constituição da República:

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (BRASIL, 2019).

O trâmite da proposta fez com que a Constituição da República incorporasse ao seu texto e reconhecesse expressamente um direito que antes era visto de modo implícito. Assim, denota-se que “a experiência legislativa segue justamente nessa direção, confirmando como é impossível prescindir de uma estratégia institucional articulada e integrada” (RODOTÀ, 2008, p. 81), devendo constituir efetiva atuação estatal na gestão e criação dos mecanismos necessários de regulação das práticas do ambiente da informação, que transcendem as fronteiras e a soberania de qualquer Estado, sendo a proteção desse direito em âmbito constitucional efetiva possibilidade de uma proteção articulada e integrada, como pretendia Rodotà.

O autor italiano ainda afirma que “a proteção de dados estabelece regras sobre os mecanismos de processamento de dados e estabelece a legitimidade para a tomada de medidas – *i.e.* é um tipo de proteção dinâmico, que segue o dado em todos os seus movimentos” (RODOTÀ, 2008, p. 17). Nesse sentido, é possível verificar que:

---

<sup>29</sup> Destaca-se, como já é de conhecimento geral, que os direitos fundamentais não são absolutos e permitem relativização, notadamente nas situações concretas quando diante de uma colisão, para os quais existem técnicas interpretativas, como a ponderação, para propor soluções. No entanto, importante referenciar que sempre se deve ter em conta o princípio matriz da dignidade da pessoa humana, balisando a interpretação em concreto.

A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática. [...] A facilidade de acesso aos dados pessoais, somada à velocidade do acesso, da transmissão e do cruzamento de tais dados, potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social.” (SARLET; MARINONI; MITIDIERO, 2017, p. 472).

Diante disso, é possível afirmar que o novo “direito fundamental exorbita aquele protegido pelo direito à privacidade, pois não se limita apenas aos dados íntimos ou privados, ao revés, refere-se a qualquer dado que identifique ou possa identificar um indivíduo” (MENDES; FONSECA, 2020, p. 473), lembrando-se sempre que o aspecto do dado não se relaciona com o aspecto de um direito de propriedade, mas da própria individualidade da pessoa, ou seja, de sua personalidade.

Nesse sentido, denota-se que o âmbito de proteção do direito fundamental de proteção dos dados pessoais engloba o direito de acesso e conhecimento dos dados, possibilidade de não conhecimento e não serem utilizados os dados pelo Estado ou terceiros, conhecimento de quem são os responsáveis pelas operações envolvendo os dados da pessoa, conhecimento da finalidade, direito de retificar e excluir os dados (SARLET; MARINONI; MITIDIERO, 2017, p. 473-474). Essas previsões, inclusive, estão constantes na Lei Geral de Proteção de Dados, reforçando o aspecto protetivo à pessoa no ambiente digital.

Importante destacar que a separação da privacidade e proteção de dados não é novidade no âmbito global, tendo em vista que, a exemplo da Carta de Direitos Fundamentais da União Europeia já mencionada, a proteção de dados é tida como direito fundamental próprio, diverso dos demais (RODOTÀ, 2008, p. 175), em um movimento tendente a dar proteção jurídica própria aos dados pessoais, uma vez que é tamanha sua relevância na sociedade.

Trata-se, ainda, de um direito fundamental que opera em uma dupla dimensão: a dimensão subjetiva, na qual o indivíduo delimita a intervenção estatal, ou seja, trata-se do aspecto de não intervenção do Estado na esfera individual; e a dimensão objetiva, onde há o dever do Estado de promover mecanismos que assegurem esse direito (MENDES; FONSECA, 2020, p. 473-474), cujo exemplo é a regulação através da Lei Geral de Proteção de Dados e outras políticas públicas

possíveis<sup>30</sup>.

A caracterização da proteção de dados como direito fundamental contribui para o fenômeno da “constitucionalização da pessoa” (RODOTÀ, 2008, p. 17), cuja extensão e alcance decorre da própria noção e conceito de dignidade da pessoa e da sua liberdade em desenvolver a personalidade humana, posto que a “inviolabilidade da pessoa deve ser reconfigurada e reforçada na dimensão eletrônica” (RODOTÀ, 2008, p. 19).

Além disso, há que se destacar a necessária proteção do desenvolvimento da pessoa a partir dos meios tecnológicos e de possíveis conflitos que surgem a partir de então, demonstrando a necessidade de uma adequada proteção. Conforme Leal

Nos dias atuais, os aspectos da tutela da privacidade e intimidade encontram-se muito integrados com a proteção de dados pessoais, pelo fato de que tais dados representam pressupostos irrenunciáveis ao desenvolvimento da pessoa humana e, ao mesmo tempo, estão conectados com demandas de mercado, pois alimentam infundáveis segmentos de atividades industriais e comerciais que pagam valores imensos por informações de seus consumidores, formatando-se, neste âmbito, zonas de potenciais conflitos entre interesses distintos (LEAL, 2020, p. 366).

Afirma-se, portanto, que o direito fundamental à proteção de dados pessoais possui um âmbito de proteção próprio que também se evidencia na dimensão objetiva, gerando o dever estatal de tutela, já estudado no capítulo anterior. Sarlet pontua que “ao Estado incumbe um dever de proteção a ser concretizado mediante prestações normativas e fáticas, notadamente, por meio da regulação infraconstitucional dos diversos aspectos relacionados às posições jusfundamentais” (SARLET; MARINONI; MITIDIERO, 2017, p. 474).

Dentre as prestações estatais, Sarlet exemplifica a previsão no ordenamento jurídico do *habeas data* e a criação de órgão para vigilância do sistema de proteção de dados (SARLET; MARINONI; MITIDIERO, 2017, p. 474), conforme já previsto na Lei Geral de Proteção de Dados Pessoais mediante a criação da Autoridade Nacional de Proteção de Dados Pessoais.

---

<sup>30</sup> No ponto, importante destacar diversos outros mecanismos protetivos previstos antes mesmo da Lei Geral de Proteção de Dados, quais sejam o Código de Defesa do Consumidor e o regramento sobre o *habeas data*, por exemplo. Ademais, é possível enunciar o próprio Marco Civil da Internet, que introduziu, no Brasil, mas fortemente a questão dos dados pessoais. No mesmo sentido, pode-se citar o anteprojeto de LGPD-Penal, que será oportunamente trabalho, que constitui, assim como a LGPD, um verdadeiro sistema jurídico da matéria.

Nesse sentido, a matéria é fortemente sensível e não se confunde com a proteção já conferida pela privacidade. Esse novo panorama, portanto, inovou a ordem constitucional com sua consideração como direito fundamental, como ocorreu com o Supremo Tribunal Federal no julgamento das ADI's 6.387, 6.389, 6.388, 6.390 e 6.393 (BRASIL, 2020). Dentro desse contexto, a partir do julgado é possível afirmar que

O amplo acesso aos dados pessoais dos cidadãos brasileiros exige, no mínimo, balizas jurídicas claras e seguras quanto a essa coleta ou transferência, a partir da previsão de medidas de segurança e critérios de intervenção proporcionais à gravidade da restrição a esse direito fundamental (MENDES; FONSECA, 2020, p. 474).

Assim, geraram-se iniciativas legislativas no âmbito ordinário, com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. A LGPD, promulgada em 2018, regula “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado” (BRASIL, 2018), demonstrando que “a proteção de dados pessoais no ordenamento jurídico brasileiro somente se estruturou em torno de um conjunto normativo unitário muito recentemente” (DONEDA, 2019, p. 259).

Por meio das dez bases legais, que disciplinam a possibilidade de alguém operar com dados pessoais, que serão vistas em momento posterior, a legislação pretende regular o tratamento de dados, a fim de se conferir a adequada proteção às liberdades no ambiente digital, eis que, dentre seus fundamentos, se encontram as liberdades de expressão, informação, comunicação e opinião, além do livre desenvolvimento da personalidade e dignidade do usuário (BRASIL, 2018).

Dentre as bases legais previstas, há que se conferir especial destaque ao consentimento e sua relação com o direito fundamental em estudo. Isso porque é ele a expressão da liberdade do indivíduo e tal disciplina “não deve ser tratada sob um perfil negocial e deve ter como orientação a atuação do poder de autodeterminação informativa da pessoa e da consideração dos direitos fundamentais em questão” (DONEDA, 2019, p. 329).

Normalmente, as formas de tratamento, coleta e utilização dessas informações são realizadas sob o argumento da utilização para execução contratual ou com o próprio consentimento do usuário, que, para ter acesso ao serviço, acaba aceitando as condições. Todavia, a lição de Rodotà é de que “o problema dos

excessos na coleta de informações e dos abusos na sua utilização pode ser enfrentado com técnicas que não confiem somente no consentimento dos interessados.” (RODOTÀ, 2008, p. 81), ou seja, mediante a utilização de instrumentos jurídicos e tecnológicos que efetivamente protejam o usuário, mesmo que este tenha dado seu consentimento. Contudo, como visto acima, o papel do consentimento tem sido muito discutido, nomeadamente por ser ele a expressão de liberdade do indivíduo sobre o tratamento de dados.

No mesmo sentido, a legislação prevê a criação da Autoridade Nacional de Proteção de Dados Pessoais, que possui um amplo rol de competências, a exemplo da elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade, atentar para a observância da proteção dos dados pessoais, fiscalizar e sancionar eventuais tratamentos de dados realizados à burla da legislação, entre outros (BRASIL, 2018). Portanto, observa-se que criação da autoridade é fator de suma importância para a proteção dos dados e observância do dever estatal de tutela do direito fundamental.

As iniciativas legislativas auxiliam, justamente, a coibir mecanismos que interfiram no exercício da liberdade do usuário na internet, tolhida por instrumentos como a vigilância, *profiling*, mecanismos que induzam à concordância imediata de políticas de privacidade, limitando o livre acesso do usuário a conteúdos diversos, figurando como verdadeiros limitadores, no aspecto subjetivo dos limites, do exercício do direito fundamental à liberdade. Salienta-se que “assume crescente relevo o problema da colisão de tais direitos com outros direitos fundamentais, notadamente no âmbito da assim chamada ‘sociedade de vigilância’ e no ambiente da internet” (SARLET; MARINONI; MITIDIERO, 2017, p. 475).

Entretanto, mesmo a questão acerca da regulamentação pela via legislativa tem sido, de há muito, objeto de debate. Essa questão é ponto nevrálgico quando se está a estudar o uso de dados pessoais e a disciplina legal, considerando o uso de dados como forma de exploração econômica e o direito fundamental à proteção de dados, correspondente a políticas públicas para assegurar esse direito. A doutrina sobre a matéria, por muito tempo, se dividia nas ideias de regulação estatal e autorregulação realizadas pelas empresas. No entanto, Sombra (2019, p. 70) aponta para quatro modelos possíveis envolvendo o tema regulação: regulatório estatal, regulatório setorial, corregulação e autorregulação. O modelo regulatório estatal consistiria

no modelo em que o Estado assumiria o papel central de regulamentar o uso de dados pessoais, sendo definido como

aquele no qual são elaboradas normas gerais de proteção de dados, aplicáveis tanto ao setor público quanto privado e usuários, mediante a criação de um órgão governamental ou um órgão responsável pela fiscalização e imposição de sanções aos agentes que descumprem as referidas normas (SOMBRA, 2019, p. 71).

A ideia de modelo regulatório setorial é semelhante ao regulatório estatal, mas como diferencial, permite, em alguma medida, a elaboração de códigos de conduta, além de englobar diversas normas editadas para o setor privado e público “com a possibilidade de diversas agências e órgãos atuarem na fiscalização e imposição de sanções aos agentes que descumprem as referidas normas, a depender da natureza do setor da economia envolvido” (SOMBRA, 2019, p. 72).

De outro lado, o modelo de correção possibilita que o Estado elabore diretrizes gerais sobre o tratamento de dados pessoais, prevendo proteções mínimas, ao passo que o ente privado poderá criar códigos de conduta, normas internas e padrões de proteção, que são validados pelos órgãos fiscalizadores posteriormente (SOMBRA, 2019, p. 73). Em grande parte, assemelha-se ao modelo adotado pelo Brasil e pela Europa para o tratamento de dados, o que se verá em momento posterior.

Por fim, no modelo de autorregulação, que se entende já superado, as empresas/iniciativa privada são as responsáveis pela elaboração das normas e códigos de conduta sem intervenção estatal ou sendo ela a mínima possível. Sombra (2019, p. 75) traz algumas críticas a esse modelo:

O êxito dos instrumentos de autorregulação é imprevisível e bastante variável a depender do setor, país e condições de implementação. A rigor, dependem de um conjunto de fatores políticos, organizacionais, culturais, tecnológicos e econômicos, o que não necessariamente indica se tratar de um modelo de pluralismo jurídico, tal como sustentado nessa tese. Sem a presença de um arcabouço regulatório com capacidade de impor sanções e assegurar o efetivo equilíbrio entre tutela dos dados pessoais e fomento à inovação, a autorregulação padece de constante desconfiança.

Em verdade, trata-se de assunto que deve ser visto com delicadeza, levando em consideração a eficácia horizontal dos direitos fundamentais, cuja observância deve ser de todos os atores sociais. Defende-se que, diante de um direito fundamen-

tal e de um dever estatal de tutela, os modelos regulatórios devem ser pautados por uma atuação firme do Estado, na busca da proteção aos direitos fundamentais que envolvem o tratamento de dados pessoais, sobretudo no tratamento de dados pelo próprio Estado e pelos grandes agentes do mercado. Decorre disso a existência de bases legais que autorizam, tão somente nessas hipóteses, as operações envolvendo dados pessoais.

Nesse sentido, afirma-se que a tutela dos dados pessoais deve ser pautada por garantias mínimas a se compensar a vulnerabilidade existente entre o usuário/pessoa e os agentes da economia digital, o que perpassa por se analisar uma perspectiva constitucional da proteção de dados (VIANA; MONTENEGRO, GLEIZER, 2020, p. 6). Os mesmos autores, quando analisam o tratamento de dados pessoais pelo Estado, referem que um direito à proteção de dados

não pode significar apenas proteção *dos* dados, deve implicar também proteção *contra* os dados, ou seja, contra os efeitos das informações que contêm para seus titulares. Sendo assim, a regulação da proteção de dados no setor público deve ser resultante entre os legítimos interesses individuais e os efeitos estatais pretendidos com o tratamento de dados pessoais. É preciso incluir, portanto, nessa ponderação as *pretensões* do Estado no exercício de suas atividades próprias (VIANA; MONTENEGRO, GLEIZER, 2020, p. 3) [grifo do autor].

Outro exemplo necessário de ser debatido nessa seara é o relativo a nominada LGPD-Penal, que se trata, ainda, de anteprojeto de lei. Conforme narrado, o projeto de lei tem o objetivo regular as operações envolvendo dados pessoais “por autoridades competentes para atividades de segurança pública e de persecução penal, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2019).

Nesse sentido, propõe-se que o Estado deva observar as normas pertinentes aos dados pessoais durante a persecução penal, a fim de reduzir a vigilância estatal e assegurar direitos ao cidadão, notadamente o investigado, bem como durante a execução de ações voltadas à segurança pública. Ponto inovador é a criminalização da transmissão ilegal de dados pessoais, o que evidencia que a tutela penal também é consequência do dever estatal de tutela aos dados pessoais e de políticas regulatórias. A temática será abordada com maior profundidade no momento oportuno, ainda mais quando se está a se falar em relações penais, que

afetam, conseqüentemente, a liberdade, e dados pessoais.

Conferir uma adequada proteção de dados, especialmente pelo seu caráter de direito fundamental, aliado as disposições previstas na Lei Geral de Proteção de Dados Pessoais visa deixar clara a proteção constitucional dada à pessoa, buscando a efetividade do macroprincípio constitucional, protegendo a personalidade humana “sem que intervenções externas e constitucionalmente ilegítimas comprometam o exercício pelas pessoas de sua liberdade e da possibilidade de terem controle sobre os próprios dados” (SARLET; SAAVEDRA, 2020, p. 53).

Diante disso, observa-se que a temática, enquanto questão jusfundamental de extrema importância, ainda tem sido relegada tão somente a uma análise estrita sobre a Lei Geral ou outras legislações ordinárias, mesmo considerando que a proteção de dados pessoais não se caracteriza pela proteção do dado em si, mas de diversas dimensões do indivíduo e de seus direitos, principalmente fundamentais, no âmbito da sociedade da informação. Entretanto, antes de se iniciar com maior profundidade os fatores de risco à liberdade, importa visualizar e analisar os elementos e instrumentos da Lei Geral de Proteção de Dados Pessoais para se entender como eles podem operar na proteção da liberdade e do novel direito fundamental.

### **3.2 Considerações sobre o sistema jurídico brasileiro de proteção de dados pessoais**

Analisado o conceito sobre o direito fundamental à proteção de dados pessoais, necessário se analisar alguns aspectos sobre a Lei Geral de Proteção de Dados Pessoais. Como antes referido, é possível visualizar que a lei não apenas visa proteger o dado pessoal, mas, na verdade, o próprio indivíduo e sua personalidade, ainda mais no ambiente digital e da Sociedade de Risco. Opera-se, nesse contexto, o dever de proteção estatal ao direito fundamental, mediante a criação de políticas públicas necessárias para a tutela desse direito por meio da regulação sobre o tratamento de dados pessoais.

Gize-se que a regulamentação sobre os dados pessoais não é temática recente, considerando as previsões normativas sobre o *habeas data*, o Código e Defesa do Consumidor e o Marco Civil da Internet. À vista do problema de pesquisa pro-

posto, que objetiva um aprofundamento maior nos instrumentos previstos na Lei Geral de Proteção de Dados Pessoais, tais diplomas serão apenas brevemente abordados, mas o que não significa desmerecer as conquistas que tais legislações trouxeram<sup>31</sup>.

O Código de Defesa do Consumidor foi um dos primeiros instrumentos legislativos a tratar sobre dados pessoais e bancos de dados nas disposições do artigo 43, sobre direitos e garantias em informações pessoais. Trata-se, essencialmente, de previsões da legislação consumerista para, na verdade, proteger o consumidor e seus dados, cuja proteção ocorre de modo acidental, haja vista a vulnerabilidade do consumidor. Entretanto, apesar dos nítidos avanços com essa legislação, promulgada na década de 90, denota-se que sua tutela, em relação aos dados pessoais em si, não é ampla, preocupando-se mais com o uso de dados e informação nas relações onde há a incidência de uma relação de consumo (DONEDA, 2019, p. 267).

O mecanismo constitucional do *habeas data* está previsto no inciso LXXII do artigo 5º da Constituição (BRASIL, 1988) e se encontra regulamentado pela Lei nº. 9.507/97, objetivando que seja permitido o acesso e o conhecimento sobre registro e armazenamento de dados que dizem respeito ao titular dessas informações em âmbito público, possibilitando, inclusive, a sua retificação (BRASIL, 1988). Trata-se de instrumento judicial que foi pioneiro na América Latina, apesar de sua pouca efetividade no Brasil. Doneda (2019, p. 287) aponta para uma função simbólica desse instrumento, haja vista as críticas por sua pouca repercussão prática nos tribunais, apontando o autor, inclusive, a sua existência como um fator negativo, posto que a sua efetividade é obnubilada pela função simbólica.

Em boa medida, Doneda (2019, p. 287-288) acentua que a sua efetividade não se consolidou em razão da dificuldade de se estruturar precocemente um sistema de proteção de dados pessoais e pelo fato de que a discussão em torno do *habeas data* se deslocou para o campo processual ao invés de sua efetividade material como garantia na proteção do dado pessoal. Afirma o autor sobre a possibilidade de se redefinir o papel *habeas data*, seja através da sua pluralização ou relegar um papel básico para os direitos de acesso e retificação de dados, criando-se um instru-

---

<sup>31</sup> O enfoque aqui proposto, como se extrai do problema de pesquisa, é tratar especialmente sobre o direito fundamental e a LGPD, de modo que não se mostra necessário maior aprofundamento nas legislações precedentes, posto que tratavam do tema ou indiretamente ou com pouca profundidade. No entanto, não se desconsidera a importância histórica e jurídica.

mento próprio para a proteção de dados em sua forma mais ampla (DONEDA, 2019, p. 288)<sup>32</sup>.

A pouca efetividade dos dois mecanismos legislativos é decorrente em grande parte do fato da Internet e das tecnologias hoje existentes serem pouco desenvolvida à época das legislações, motivo pelo qual sua proteção restou pouco difundida para os dias atuais.

Ou seja, as legislações acima vistas não levaram em conta aquilo que Beck chamou de metamorfose digital, caracterizado pelo entrelaçamento do on-line e do off-line (BECK, 2018, p. 190), noção que, atualmente, se revela de suma necessidade frente aos riscos surgidos desse ambiente. Denota-se, nesse sentido, que os riscos do ambiente digital não se constituem somente na ordinariade, para os quais se constroem remédios jurídicos para que sejam evitados, mas no âmbito extraordinário, ou seja, uma vez acontecidos danos decorrentes desses riscos, suas consequências tornam irrecuperável o status anterior.

Importante destacar que, no Brasil, as legislações sobre a proteção de dados são recentes e a estrutura de um sistema que os proteja é igualmente recente e se constroi pouco a pouco de forma mais unitária. Em grande parte, o sistema de proteção brasileiro e o próprio direito à proteção de dados decorreu das disposições de direitos fundamentais previstas na Constituição da República, “cuja relação, propósito e alcance são fornecidos pela leitura da cláusula geral da personalidade” (DONEDA, 2019, p. 259)

Nesse cenário, considerando a necessidade de regulamentação inclusive sobre a própria Internet, o Marco Civil da Internet surgiu como promissora legislação. Trata-se de uma das primeiras legislações brasileiras a dispor, de forma mais sistematizada, sobre a regulação da internet, iniciando no país uma nova fase no que tange aos direitos do usuário na internet. Tal legislação “denota a transformação do pensamento e os esforços do legislador brasileiro para regulamentar o uso da Internet com o estabelecimento de princípios, garantias, direitos e deveres” (CRESPO; RIBEIRO FILHO, 2019, p. 171).

Além disso, “inevitavelmente a instituição do Marco Civil da Internet também trouxe ao meio jurídico o debate sobre a necessidade de uma norma jurídica que

---

<sup>32</sup> Em grande medida, conferir novamente a importância jurídica ao *habeas data*, remodelando-o para os novos cenários, permitirá a efetivação judicial do direito fundamental à proteção de dados, ampliando-se os instrumentos de sua proteção para além daqueles previstos na LGPD.

recepcionasse e reconhecesse direitos, dentro do contexto da internet no Brasil” (FORTES, 2016, p. 120).

Dentre todas suas previsões, importa destacar o amparo principiológico previsto no artigo 3º, com especial enfoque aos princípios da proteção da privacidade e dos dados pessoais, onde o documento legal fundamenta o direito à privacidade como necessário para utilização da internet (FORTES, 2016, p. 127), além de assentar o a neutralidade da rede<sup>33</sup> como um de seus fundamentos.

Nesse sentido, é possível afirmar que “acertou o Legislador ao estabelecer um regime jurídico de proteção de dados pessoais no âmbito da regulamentação do uso da internet no país.” (MENDES, 2016, p. 38), tendo em vista que a lei adiantou-se na disciplina das informações dos internautas, prevendo regramentos mínimos para as operações envolvendo dados pessoais (FORTES, 2016, p. 128). Ou seja, a lei que norteia a Internet no Brasil, apresenta parâmetros mínimos de observância no tratamento de dados, de forma que todas as legislações devem observar os seus regramentos.

Além disso, “o Marco Civil dá ênfase à proteção dos dados pessoais, informações que podem identificar uma pessoa e que comumente são utilizadas ou requeridas pelos provedores de acesso à internet ou provedores de serviços no Brasil” (JESUS; MILAGRE, 2014, p. 22). Nesse cenário, foi legislação inovadora nesse quesito, haja vista que, até então, não se falava em uma proteção jurídica mínima aos dados pessoais.

Dentre outros principais pontos de avanço do Marco Civil da Internet, é recepcionado o consentimento, de forma expressa, sobre a coleta, uso, armazenamento e tratamento de dados pessoais, abrindo, inclusive, a “possibilidade de exclusão definitiva dos dados pessoais que tiverem sido fornecidos para determinada aplicação de internet, a requerimento do interessado” (FORTES, 2016, p.128), sendo que aqueles que violarem os dados pessoais poderão também ser responsabilizados.

A disciplina do consentimento, como visto anteriormente, é ponto nevrálgico quando se fala da relação proteção de dados pessoais e liberdade, de modo que é o consentimento a baliza entre a disponibilidade ou não de se tratar os dados pessoais

---

<sup>33</sup> O papel da neutralidade da rede e os debates havidos sobre se adotar a neutralidade da rede extrapolam os limites do presente trabalho, considerando a ampla discussão em torno desse princípio. Contudo, são válidas as lições trazidas por Fortes (2016) em sua obra, a qual se remete as lições para maior aprofundamento.

ou mesmo de se falar em direito indisponível, caso essa equação balance para uma desvalorização do consentimento e maior proteção. Trata-se de ponto fundamental, cujos contornos serão aprofundados no momento oportuno.

Apesar dessas inovações trazidas, o Marco Civil da Internet “trouxe a necessidade de regulamentação de dispositivos específicos como é o caso da seção que trata da proteção da privacidade e dos dados pessoais na rede” (FORTES, 2016, p. 172), o que é tido de modo expresso pela legislação. No mesmo sentido das legislações mundiais, a proteção de dados, especialmente no ambiente informático, exige sua regulamentação através de lei específica. Veja-se que

Na oportunidade, o legislador houve por bem sedimentar a proteção à privacidade e trouxe um capítulo exclusivo para a salvaguarda dos dados pessoais, cuja aplicação, contudo, depende do uso da internet. Ainda que a referida Lei não estivesse voltada, fundamentalmente, à autonomia dos dados pessoais, sua contribuição foi de grande valia (CRESPO; RIBEIRO FILHO, 2019, p. 171).

Dessa maneira, denota-se que há a necessidade de se estabelecer um sistema jurídico íntegro, que perpassa não somente pelas legislações acima estudadas, mas de uma Lei Geral que apresente parâmetros gerais e procedimentais no tratamento de dados pessoais. Como pontua acertadamente Danilo Doneda (2019, p. 24) é “necessário que o ordenamento jurídico estabeleça critérios proporcionais de tutela da pessoa nesta área, que é muito fortemente ligada ao desenvolvimento da tecnologia”, considerando que “a internet constitui um ambiente de exercício de diversos direitos fundamentais [...] a proteção da privacidade e dos dados pessoais apresenta-se como um pressuposto para o exercício desses direitos”. (MENDES, 2016, p. 38).

É esse cenário que faz acentuar a importância proteção de dados pessoais dos usuários, especialmente mediante a criação dos instrumentos jurídicos mínimos que possibilitem a salvaguarda dos internautas.

Vale destacar que a preocupação legislativa já vem de décadas no continente europeu, criando-se marcos normativos acerca da proteção de dados, a exemplo da Convenção 108, de 1981, do Conselho da Europa, da Diretiva 95/46/CE e do Regulamento Geral de Proteção de Dados da União Europeia, inclusive em caráter de direito fundamental. Do mesmo modo, ao longo do tempo foram promulgadas diversas iniciativas legislativas dos países nessa temática, a exemplo da Lei 78-17, denominada *Informatique et Libertés*, e 1978, na França; da Lei do *Land* alemão de

Hesse, em 1970, na Alemanha; *Datenschutzgesetz*, Lei nº. 565/1978, da Áustria; da Lei de Proteção de Dados Pessoais n.º 25.326, de 2000, na Argentina; entre outros.

É sabido que a Lei Geral de Proteção de Dados Pessoais é fruto de um movimento mundial para se robustecer o tratamento de dados, notadamente a partir da criação das tecnologias da informação, cujo alcance é global (CASTELLS, 2003, p. 08). Tal fato se deve, principalmente, em razão de que os novos meios de comunicação oriundos da sociedade em rede vão na contramão da preservação da privacidade das pessoas, oferecendo, na verdade, obstáculos para os usuário assumirem o controle das informações que delas são extraídas (RUARO; GLITZ, 2019, p. 342).

Em certa medida, o surgimento de uma lei específica que verse sobre dados pessoais no Brasil é fruto de questões econômicas decorrentes da promulgação do RGPD. Isso porque o RGPD prevê a impossibilidade de negociação entre empresas europeias com empresas sediadas em países que não possuíam regulamentação condizentemente suficiente aos padrões europeus (LIMA, 2020, p. 234).

Nesse sentido, há um movimento crescente pela padronização mundial nas previsões sobre tratamento de dados, notadamente para sua circulação internacional, dentro de um modelo ideal que uniformize as leis de proteção e modelos regulatórios (LIMA, 2020, p. 238), temática que será trabalhada no tópico seguinte, visto as suas relações com o direito de liberdade.

Nesse cenário é que surge a Lei Geral de Proteção de Dados Pessoais, qual seja a Lei nº. 13.709, promulgada em 2018, atendendo a uma exigência já existente no Marco Civil da Internet em seu artigo 3º, inciso III. A LGPD<sup>34</sup> visa disciplinar “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018), apresentando inovadoras disposições sobre a proteção de dados, segurança na rede, governança digital, além da criação

---

<sup>34</sup> Vale aqui, novamente, trazer a ressalva já feita de que não se ignora uma proteção prevista no Código de Defesa do Consumidor no tocante aos bancos de dados dos consumidores e na Lei do *Habeas Data*. Nesse sentido, “no Código de Defesa do Consumidor, a Seção VI do Capítulo V é dedicada aos bancos de dados e cadastros de consumidores e tem no art. 43 o seu principal dispositivo. Ele garante o acesso às informações arquivadas sobre o consumidor e suas respectivas fontes, além de estabelecer um prazo máximo da permanência delas no cadastro, o dever de informar sua abertura e de proceder à imediata correção de informações falsas ou equivocadas, a pedido do consumidor” (OLIVEIRA; LOPES, 2019, p. 67). Todavia, considerando o enfoque pretendido, limita-se ao já referido anteriormente, considerando a proposta do presente texto.

da Autoridade Nacional de Proteção de Dados Pessoais<sup>35</sup>.

Fortemente inspirada pelo Regulamento Geral de Proteção de Dados europeu<sup>36</sup>, a lei brasileira ascendeu ainda mais o debate acerca da proteção de dados pessoais, trazendo inovações, conceitos e regramentos referentes ao tratamento de dados no Brasil. Observa-se que a lei conceitua dado pessoal como a “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018), além de categorizar como dado pessoal sensível o “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” (BRASIL, 2018)<sup>37</sup>.

Em síntese, o âmbito de proteção do dado pessoal sensível é mais específico e com maiores regramentos, exigindo especial atenção por parte do agente de tratamento, dada a natureza dessas informações. Dentre as suas diferenças, denota-se bases legais diversas, com especial destaque ao consentimento.

Além disso, um dos principais pontos é o conceito conferido ao tratamento de dados pessoais, que é

[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

Em resumo, o tratamento – aqui se tratando em relação aos dados de meios

---

<sup>35</sup> Aqui, defende-se que a Autoridade Nacional assume um dos papéis mais relevantes na proteção da liberdade no ambiente digital e sua relação com dados pessoais, posto o seu papel de agente fiscalizador, regulamentador, bem como de elaborar diretrizes para uma Política Nacional da Privacidade e dos Dados Pessoais (BRASIL, 2018).

<sup>36</sup> Ruaro e Glitz (2019, p. 346) acertadamente ressaltam: “A legislação europeia foi a grande norteadora da Lei Geral de Proteção de Dados Pessoais no Brasil, servindo de grande inspiração e refletindo importantes contribuições em nossa lei. Porém, o ponto mais emblemático desta inspiração legislativa está justamente no fato da diferença cultural existente entre a União Europeia e o Brasil. A comunidade europeia possui uma cultura de preservação da sociedade [...]. Em contrapartida, a população brasileira possui uma cultura bastante distinta da europeia, na qual o titular dos dados, por exemplo, não vê mal algum em fornecer o número de seu CPF para obter um mísero desconto em uma farmácia”. Ou seja, a diferença entre os instrumentos protetivos europeu e brasileiro não somente se efetiva com a atuação dos órgãos, mas também de uma cultura de proteção de dados pessoais.

<sup>37</sup> Os dados pessoais sensíveis têm uma intrínseca relação com o direito de liberdade. Por seu conceito, qualquer indevido tratamento de dados, vazamento ou outro procedimento que possa trazer danos ao seu titular, afeta, mesmo que indiretamente, a liberdade pessoal, pois as questões que envolvem opiniões políticas, raça ou cor, por exemplo, são passíveis de discriminação, invadindo a seara da dignidade da pessoa. No tocante às opiniões políticas, é interessante o paradoxo que Rodotà aponta e que será visto mais adiante.

digitais – contempla, por exemplo, qualquer tipo de cadastro, solicitação de serviços, consumo de mídias pela internet, para o qual é necessário o uso das informações ao provedor, demonstrando a verdadeira amplitude daquilo que é o tratamento feito na rede pelos provedores de aplicação. Além disso, com essa forma de operação das informações em meios digitais, Doneda (2019, p. 151) pontua uma “mudança qualitativa no tratamento dos dados pessoais, à qual aludimos, baseia-se na utilização de novos métodos, algoritmos e técnicas”, sendo, dentre essas técnicas, a do *profiling*<sup>38</sup>, que consiste em traçar o perfil do usuário, comumente utilizado para mapear gostos e interesses do usuário, com o objetivo de qualificar a prestação do conteúdo.

Nesse sentido, observa-se que a disciplina sobre o tratamento de dados pessoais em muito respeita ao princípio da reserva legal. Ou seja, apenas haverá tratamento de dados pessoais quando expressamente autorizado por lei. Tratando-se de temática afeta aos direitos fundamentais, quando há intervenção informacional, ou seja, intervenção em algum dado ou informação do indivíduo, caracterizando alguma restrição ao seu direito, somente pode se estar amparado por lei. Daí a importância da lição abaixo:

Se intervenções (informacionais) precisam estar autorizadas em lei, também é claro que apenas aquilo que se pode compreender da leitura da norma autorizativa pode, de fato, estar autorizado. Por essa razão, é atributo da reserva de lei o chamado *imperativo de determinação e clareza*: é necessário autorizar expressamente a ação naturalística (interceptar, infiltrar, armazenar etc.) em si, ou seja, não bastam previsões gerais do estilo “métodos para obtenção/tratamento de informações” (VIANA; MONTENEGRO, GLEIZER, 2020, p. 56) [grifo do autor].

Desse modo, a LGPD traz dez bases legais para o tratamento de dados pessoais, tido, no presente trabalho, como taxativos, quais sejam: consentimento; cumprimento de obrigação legal; execução de políticas públicas pela Administração; estudos por órgãos de pesquisa; execução contratual; processos judiciais, administrativos e arbitrais; proteção da vida e integridade física; tutela de saúde; legítimo interesse do controlador; proteção do crédito (BRASIL, 2018). Dentre todos eles, é inevitável que se assuma maior relevância ao consentimento.

Apesar de já ter sua previsão no Marco Civil da Internet, a Lei Geral traçou

---

<sup>38</sup> O *profiling* é ponto importante a ser observado quando se fala de proteção de dados pessoais. A regulação do tratamento em muito visa mitigar e dar garantia à pessoa em face dos instrumentos de perfilação, a partir das previsões das bases legais e aspectos procedimentais.

contornos mais específicos sobre o instituto do consentimento, definindo-o como a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018), tratando-se de um ato unilateral do titular, vinculado, normalmente, à disposição contratual (DONEDA, 2006, p. 378). Alguns autores, e mais adiante se visualizará, abordam a questão da figura do mito do consentimento, de forma que seria ele um procedimento meramente acessório no tratamento de dados. Contudo, é inevitável se afirmar a sua importância na economia informacional.

Conectado com o fundamento da autodeterminação informativa, previsto no artigo 2º, inciso II, “o consentimento do titular dos dados recebeu tutela destacada na LGPD, ainda que não seja, vale lembrar, a única hipótese legal para o tratamento de dados pessoais nem hierarquicamente superior às demais” (TEPEDINO; TEFFÉ, 2019, p. 297-298). É inegável, no entanto, o papel assumido pelo instituto com a promulgação da lei, frente as suas demais disposições, uma vez que se denota a “ênfase atribuída ao consentimento, seguindo a linha do regulamento europeu e das normas mais atuais sobre o tema, além de uma série de disposições que oferecem regramento específico para concretizar, orientar e reforçar o controle dos dados através do consentimento” (TEPEDINO; TEFFÉ, 2019, p. 298).

Para Danilo Doneda (2006, p. 377), a importância do instituto “reside na possibilidade de autodeterminação em relação aos dados pessoais, e que esta autodeterminação deve o elemento principal a ser levado em conta para caracterizarmos tanto a natureza jurídica bem como os efeitos deste consentimento”. Entretanto, o autor adverte dois pontos a serem observados quando se está a analisar o consentimento: a utilização dele com o caráter meramente acessório, ligado a uma situação fundamental; e que seja ele um procedimento inócuo (DONEDA, 2019, p. 298-299)<sup>39</sup>.

Ressalta-se que “o confronto com situações reais revela que, em tais situações, a alternativa a não revelação dos dados pessoais pelo seu titular costuma ser uma – por vezes, brutal – renúncia a determinados bens ou serviços” (DONEDA, 2019, p. 298), fazendo com que o titular deixe de ter acesso ao aplicativo, rede social, serviço, pelo simples fato de não ter concordado com a forma de operação dos

---

<sup>39</sup> Há que se ter ressaltar quanto ao consentimento, porquanto está-se a se falar do “mito do consentimento”. O consentimento é visto, comumente, com caráter meramente acessório, o que lhe faz perder o caráter de sua importância, especialmente pelo fato de estar condicionado à fruição de determinada plataforma ou aplicação.

dados pelo provedor<sup>40</sup>.

Nesse sentido é que se diz que o consentimento deve ser informado, ou seja, o titular dos dados deve ter ciência acerca daquilo que está consentindo sobre seus dados, bem como ser advertido sobre a negativa em fornecê-lo, sendo plenamente vedado o consentimento dado de maneira genérica, nos termos do artigo 8º, §4º<sup>41</sup>. Essa necessidade de que ele seja informado serve “para evitar que seja inviabilizado pelos modelos de negócios em que se pretende impor o consentimento sem dar o efetivo conhecimento ao titular dos dados pessoais” (LIMA; RAMIRO, 2020, p. 252). Veja-se que “para diminuir a assimetria técnica e informacional existente entre as partes, exige a lei que ao cidadão sejam fornecidas informações transparentes, adequadas, claras e em quantidade satisfatória acerca dos riscos e implicações do tratamento de seus dados” (TEPEDINO; TEFFÉ, 2019, p. 301).

Todavia, importante lembrar que o consentimento não é o único meio que permite o tratamento de dados pessoais. Como afirmado anteriormente Lei Geral arrola dez hipóteses em seu artigo 7º que possibilitam que os agentes de tratamento operem com dados. Essas hipóteses de tratamento, nomeadas como bases legais, devem observar e ser lidas em conjunto com outros pontos fulcrais da LGPD, quais sejam os princípios da finalidade, adequação, necessidade e transparência do tratamento dos dados pessoais, que balizam a interpretação e as operações dessas informações.

Ressalta-se que a LGPD apresenta forte carga principiológica que, entende-se, deve servir de sustentáculo hermenêutico para suas disposições. Como bem ressalta Lima (2020, p. 196) a importância dos princípios reside na possibilidade de “formação de um sistema jurídico, proporcionando-lhe unidade científica”, ou seja, são verdadeiros norteadores das interpretações sobre questões relacionadas ao tra-

---

<sup>40</sup> Como bem já advertiu Rodotà (2008, p. 76), “o condicionamento deriva do fato de que a possibilidade de usufruir determinados serviços, essenciais ou importantes, ou tidos como tais, depende não somente do fornecimento de determinadas informações por parte do usuário do serviço, mas também do fato de que tais informações (eventualmente com base no consentimento do interessado) podem posteriormente ser submetidas a outras elaborações. Este é o caso de todos os serviços obtidos através das novas mídias interativas, cujos gestores, por evidentes razões de ordem econômica, estão prontos a exercer forte pressão sobre os usuários para que estes autorizem a elaboração (e a eventual transmissão a terceiros) de ‘perfis’ pessoais ou familiares baseados nas informações coletadas por ocasião do fornecimento dos serviços”.

<sup>41</sup> Conforme Lima e Ramiro (2020, p. 252) “a fim de corrigir tal assimetria, a LGPD determina que será nulo o consentimento manifestado de maneira genérica (art. 8º, §4º da LGPD), ou seja, o consentimento deve estar relacionado à uma finalidade específica do tratamento de dados pessoais inclusive por que assim estabelecem os princípios da finalidade, adequação e necessidade (art. 6º, inc. I, II e III da LGPD). Além disso, o consentimento fornecido por escrito deve constar de cláusulas destacadas das demais (art. 8º, §1º da LGPD)”.

tamento de dados pessoais. Como se pode observar, esses princípios estão dispostos no artigo 6º, juntamente com os outros princípios do livre acesso, qualidade dos dados, segurança, prevenção, não discriminação e responsabilização, pautando a forma de tratamento de dados pessoais (BRASIL, 2018). Faz-se uma breve exposição sobre tais princípios, de modo a se possibilitar compreender o amparo e importância que assumem em um sistema jurídico de proteção de dados, pautado pela LGPD<sup>42</sup>.

O princípio da finalidade, na destacada lição de Rodotà, é princípio que assume “particular intensidade quando os dados pessoais do usuário do serviço não são solicitados por quem oferece o serviço, mas são uma consequência quase ‘natural’ do fornecimento do próprio serviço” (RODOTÀ, 2008, p. 204). Ainda, conforme o autor, “torna-se essencial para determinar a legitimidade do uso dos dados coletados, seu tempo de conservação, a admissibilidade de sua interconexão com informações contidas em outros bancos de dados” (RODOTÀ, 2008, p. 204).

Segundo a própria LGPD, a finalidade diz respeito à “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018), não se podendo utilizar de finalidades genéricas ou imprecisas para tratamento dos dados. Nesse sentido, “os provedores de aplicações de internet não podem guardar dados pessoais que excedam a finalidade pela qual o usuário titular consentiu que armazenassem, salvo em casos específicos previstos em Lei” (FLUMIGNAN; FLUMIGNAN, 2020, p. 129).

Em sentido semelhante é previsto o princípio da adequação. Conforme a própria definição legal, a adequação é “a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (BRASIL, 2018). Apesar da semelhança com a finalidade, a adequação se encontra em uma dimensão mais objetiva, exigindo a compatibilidade do serviço ou produto com as informações coletadas (FLUMIGNAN; FLUMIGNAN, 2020, p. 130).

Por sua vez, a necessidade vem demonstrada pela restrição dos dados coletados a apenas aqueles necessários para a finalidade informada (OLIVEIRA; LOPES, 2019, p. 75). Conforme a definição dada pela LGPD, o princípio da necessida-

---

<sup>42</sup> Entende-se aqui que os princípios da legislação infraconstitucional podem servir de parâmetro hermenêutico ao direito fundamental à proteção de dados nas relações com os outros direitos fundamentais, de modo que a relação entre eles sempre se mostra presente, como já o fez o Supremo Tribunal Federal por ocasião do julgamento da ADI anteriormente mencionada.

de diz respeito à “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (BRASIL, 2018). Também há que se conferir o devido destaque ao princípio da transparência, que é a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial” (BRASIL, 2018). Por esse princípio, exemplificativamente:

[...] pode-se citar o fato de que não é possível o compartilhamento de dados pessoais com terceiros de forma oculta. Caso quem efetue o tratamento de dados pessoais deseje repassá-los a terceiros, inclusive para operadores que sejam essenciais à execução do serviço, é necessário informar e obter o consentimento do titular dos dados pessoais (FLUMIGNAN; FLUMIGNAN, 2020, p. 130).

Por esses motivos que tal princípio é um dos mais presentes na LGPD, dado que não se encontra apenas no momento da coleta, mas por toda a operação de dados (OLIVEIRA; LOPES, 2019, p. 76), podendo estar presente inclusive após a todo o tratamento das informações. Se somados todos os fatores previstos na legislação, além da importância elevada da proteção dos dados, do consentimento, da finalidade, adequação, necessidade e transparência do tratamento, verifica-se farto arcabouço protetivo do internauta no que toca às suas informações concedidas.

Ademais, a LGPD traz inúmeras disposições acerca de programas de governança e boas práticas no tratamento de dados pessoais. São pontos essenciais, que, atrelados a um direito fundamental de mesmo teor, denotam como entes privados também estão sujeitos aos ditames e regramentos, evidenciando que a opção brasileira é de um sistema integrado no que toca à proteção de dados<sup>43</sup>.

Nesse contexto, há a crucial necessidade de adequação das políticas de privacidade de empresas, provedores de conexão e aplicação, a essas previsões normativas, tendo em vista que, em razão da coleta dos dados pessoais, os usuários, pelas informações por ele fornecidas, são rotineiramente identificados pelos provedores, demonstrando os indicativos de sua personalidade (DONEDA, 2019, p. 23).

---

<sup>43</sup> Com esse entendimento, reforça-se ainda mais a tese da vinculação dos particulares aos direitos fundamentais, como no célebre Caso Lüth. Além disso, é a partir das lições de Reis (2005) que se pode afirmar o papel que os direitos fundamentais ocupam nas relações entre particulares, baseados no princípio matriz da dignidade da pessoa humana.

Imperioso referir que a Lei Geral de Proteção de Dados Pessoais institui, assim como em outros países, como a Itália, uma Autoridade Nacional de Proteção de Dados Pessoais, que se encontra submetida à Presidência da República. O modelo adotado pelo Brasil, em razão de sua estrutura, competência e modo de funcionamento, em muito se aproxima das Agências Reguladoras (LIMA, 2020, p. 253). No entanto, observa-se que um dos principais aspectos necessários para o funcionamento adequado de uma Autoridade de tamanha importância se encontra maculado, que é a independência, ponto que será abordado no tópico seguinte.

A legislação trouxe inúmeras missões e competências para a Autoridade Nacional, conferindo-lhe poderes legiferantes e judicantes, ao que alguns autores, inclusive, apontam para um possível quarto poder (LIMA, 2020, p. 256)<sup>44</sup>. Ao mesmo tempo, pode ser a Autoridade um importante órgão a garantir os direitos fundamentais dos indivíduos, mediante seus instrumentos de tutela e suas competências, previstas no artigo 55-J da LGPD. Lima (2020, p. 303) adverte que um dos principais pontos positivos é a possibilidade de uma tutela administrativa ao cidadão que entender indevido o tratamento de seus dados por alguém.

De todo modo, observa-se que a Autoridade é importante elemento a se fazer afirmar o direito à proteção de dados pessoais e a possibilitar a cultura de proteção aos dados. Nesse sentido, o próximo tópico versará sobre limites e possibilidades diante da proteção jurídica dos dados pessoais e a liberdade no ambiente digital. Inúmeros pontos do sistema brasileiro vem a reafirmar os direitos já consagrados nessa seara. Por outro lado, há que se destacar algumas limitações e desafios a serem superados para se alcançar um padrão mínimo de proteção. É o que versará o derradeiro tópico.

---

<sup>44</sup> No cenário das Agências Reguladoras ocupando o papel legiferante e judicante, há que se fazer um breve parêntese sobre o cenário vivenciado nos Estados Unidos. A crítica é de Lopes (2020, p. 168) quando afirma sobre “o imenso destaque das Agências Reguladoras, ocupando funções tradicionalmente reservadas ao Legislativo e Judiciário. Essa nova forma de produção normativa contaria com maiores capacidades técnicas e um regime de legitimação próprio para resolver conflitos em áreas específicas. As Cortes americanas têm se mostrado cada vez mais deferentes às decisões de agências reguladoras, que operam sob uma lógica diferente do raciocínio jurídico, nas quais os argumentos de princípio são analisados conjuntamente a argumentos de política”. Apesar das distintas realidades entre o Brasil e os EUA, há que se fazer a ressalva, sobretudo que, pelo preceito legal, a ANPD assumirá semelhante papel.

### **3.3 A proteção jurídica dos dados pessoais e a proteção e limites à liberdade no ambiente digital: caminhos para possibilidade da liberdade na Era da Informação e da Sociedade de Risco.**

Assentadas nos capítulos e tópicos anteriores as premissas necessárias para o debate do presente trabalho e buscar uma resposta ao problema de pesquisa proposto, impende realizar o diálogo e traçar equações e sinergias possíveis entre uma proteção jurídica aos dados pessoais e a liberdade no ambiente da Sociedade de Risco, aqui delineada como uma sociedade também decorrente desenvolvimento das tecnologias digitais, caracterizado pelo conceito de metamorfose digital.

Essa relação entre direitos e vertentes teóricas é, de fato, necessária de análise mais profunda, considerando o ambiente da Sociedade de Risco e a da importância que os meios tecnológicos assumiram e assumem nas relações sociais, uma vez que elas são marcadas “pelos mais diversos níveis de tensionalidades, envolvendo problemas de ordem econômica, política, ideológica, dentre outros, o que gera multiplicidades de conflitos de difícil equação” (LEAL, 2017, p. 39).

De outro lado, é notório o impacto que o uso de dados pessoais causou na economia. Erigiu-se um novo e promissor mercado, cujas bases se assentam no uso desses dados seja para a publicidade direcionada<sup>45</sup>, criação de novos *softwares*, mecanismos de funcionamento de aplicativos, entre outros. Ou seja, atualmente, as relações são marcadas pelo uso de dados pessoais, os quais podem ser considerados como imprescindíveis para o desenvolvimento social. Daí porque se falar em tensionalidades que envolvem múltiplos fatores de risco e que igualmente merecem a guarida legislativa<sup>46</sup>.

Esses fatores de risco (sejam os riscos econômicos que o *Big Data* pode causar, seja as influências na esfera individual) devem ser equacionados nessas relações sociais e levados em conta no aspecto legislativo. Nesse sentido, observa-se que a teoria da Sociedade de Risco aduz que os riscos ordinários não podem ser visualizados apenas como consequências comuns da modernidade, mas como efei-

---

<sup>45</sup> Conforme lição de Bioni (2021, p. 15) é “uma prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo”.

<sup>46</sup> Trata-se de uma difícil equação social, haja vista que, na atualidade, o uso de dados pessoais se torna cada vez mais evidente para o desenvolvimento de pesquisas, estratégias de mercado, entre outros, de modo que, diante do direito fundamental de tutela da pessoa, devem ser traçadas as balizas mínimas para o regular equilíbrio.

tos da modernidade e seus reflexos existenciais, cuja controlabilidade tem se mostrado insatisfatória (LEAL, 2017, p. 40). Quando se fala da realidade digital, tem-se que se trata de um risco imaterial e de difícil percepção, de forma que o Estado, diante dessa realidade, não tem se mostrado suficiente no seu controle (BECK, 2018, p. 186).

Por tal motivo, objetivar panoramas mínimos de procedimentos e proteção é se falar em uma busca na mitigação de riscos e oferecer o necessário controle das informações pessoais e aumento da consciência dos riscos (BECK, 2018, p. 185). Segundo Beck (2018, p. 187), essa perspectiva passa por encarar um dever de proteção de dados como um “supremo direito humano internacional” e encarar os riscos globais a partir de uma realidade cosmopolita (BECK, 2018, p. 189), que se visualiza pelo desafio de como ampliar a nível global os marcos regulatórios protetivos sobre dados pessoais.

Nesse sentido, um dos grandes debates sobre Estado e dados pessoais é sobre o uso estatal desses elementos e suas finalidade. Em cenários de maior risco à privacidade e aos dados pessoais, fundamenta-se a possibilidade de Estados de Exceção, baseados, por exemplo, nas questões de segurança pública, operadoras de restrições a esses direitos fundamentais. Leal (2020, p. 361) traz o exemplo do Estado de Urgência promovido na França a partir de ataques em Paris, no ano de 2015, sob o fundamento da segurança pública e nacional, onde restou autorizada a promoção acesso a domicílios sem autorização judicial e outras devassas à privacidade e dados pessoais.

A formatação de modelos persecutórios estatais baseados no tratamento de dados pessoais pode consubstanciar fator de perigo e riscos aos direitos fundamentais, se realizados de modo desmedido e sem a devida regulação, pois:

Em uma sociedade de informação com relativa centralidade no trânsito e acúmulo de dados pessoais, o modelo repressivo penal pode se associar ao modelo de parcerias preventivas de natureza tecnológico-informacional. Assim, apesar da ausência de respostas eficazes no combate à criminalidade pelo modelo repressivo, ele não só continua em expansão como pode encontrar um aliado para preencher as lacunas que poderiam indicar seu esgotamento: o modelo de parcerias preventivas (GARCIA; GONTIJO, 2021, p. 37).

Nota-se que a utilização de dados e informações para tais finalidades pode reforçar o sistema punitivo e seletivo, nomeadamente no Brasil, acarretando ainda

mais na perda da efetividade de alguns direitos, a exemplo da liberdade. Em sendo assim, exsurge a necessidade de regulamentação mínima para se balancear esses direitos, dado que a restrição a direitos fundamentais possui reserva legal, cuja proteção não é amparada pela LGPD vigente, cuja vedação está prevista no rol do artigo 4º. Gize-se que a legislação já regulamenta a questão da restrição à privacidade e de dados para a persecução em alguns aspectos, como é o caso do sigilo bancário, interceptação telefônica e telemática, cujas balizas se dão na verificação do caso concreto pelo Poder Judiciário.

Nesse sentido, há ausência de regulamentação mais robusta no campo da segurança pública, por exemplo, fator que pode gerar riscos aos direitos fundamentais diante da balança direito fundamental à segurança pública e direito fundamental a proteção de dados pessoais. Provém desse contexto a contundente crítica de Garcia e Gontijo (2021, p. 36):

Isso se dá, contudo, de modo a reforçar a seletividade do sistema punitivo – mediante a racionalização de dados racistas, por exemplo – e a ampliar a perda de direitos e garantias fundamentais. Seja por meio de videomonitoramento, mecanismos de rastreamento, perfilhamento, entre outros, fato é que as tecnologias possibilitaram a ampliação dos instrumentos à serviço da segurança pública e da persecução penal, sem, contudo, ainda vigorar uma legislação que balize de forma adequada o tratamento de dados e informações nessa seara.

Trata-se de ponto de extrema relevância na equação proteção de dados e liberdade dado os reflexos penais que existem entre o uso de dados pessoais para a segurança pública e a persecução penal. É sabido que o Direito Penal materializa o poder punitivo estatal e, desse modo, traz consequências diretas à liberdade. Nesse sentido, como já referido no decurso do presente trabalho, o anteprojeto de uma LGPD-Penal é elemento necessário de ser debatido entre Estado e sociedade. Ora, se o uso de dados pessoais por entes privados deve ser regulamentado, como já o é, nada mais lógico que regulamentar o uso de dados pessoais para as atuações estatais que mais podem mitigar a liberdade. Não somente regulamentar, mas conferir e sedimentar mecanismos protetivos nessa seara. Nesse contexto:

O termo “*proteção de dados*”, embora não seja incorreto, pode induzir a erro quando se pensa em regulação para a segurança pública e o processo penal. O erro em questão consistiria em supor que um regime de proteção de dados se inicia com um conjunto de normas e órgãos que o Estado tem de criar, para que os dados pessoais sejam adequadamente protegidos. Nesse caso, a proteção de dados seria algo semelhante à proteção

ao consumidor: um conjunto de normas e órgãos sem os quais o titular dos dados estaria suscetível a toda sorte de abusos. A tarefa do legislador, no que aqui nos interessa, consistiria em garantir esses *standards* de proteção do titular dos dados pessoais para compensar a sua vulnerabilidade; e isso especialmente em razão do advento de novas tecnologias e das possibilidades de tratamento que oferecem aos órgãos de segurança pública e persecução penal. Embora tais normas e órgãos sejam necessários, essa forma de compreender a proteção de dados ignora um aspecto fundamental do problema: o *status* constitucional dos dados pessoais (VIANA; MONTE-NEGRO, GLEIZER, 2020, p. 6).

Destaca-se que o panorama se amplia diante da Sociedade de Riscos, posto que é geradora de contextos de incerteza e, sobretudo, incredulidade nas instituições e pessoas (LEAL, 2017, p. 39). Logo, é preciso um agir estatal efetivo de forma a, primeiro, equacionar de modo adequado as relações entre dados pessoais, segurança pública e persecução penal, sem olvidar a necessária garantia do vulnerável nesse contexto, e, segundo, fixar *standards* protetivos mínimos, nomeadamente mediante o estabelecimento de procedimentos e políticas públicas, amparadas pelos direitos fundamentais.

Leal acentua, da mesma forma, que a LGPD reservou espaço a uma legislação específica nessa matéria, referindo, porém a existência de outros desafios relacionadas ao tema:

Ao mesmo tempo, em seu art. 4º, inc. III, a norma autorizou a flexibilização daqueles direitos para os fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais, sendo que o tratamento de dados pessoais previsto neste inc. III será regido por legislação específica, “que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei”. Por certo que aqui já temos outros desafios que é o de densificar materialmente – e no caso concreto – os níveis e possibilidades das *medidas proporcionais e estritamente necessárias* ao escopo da norma e diante de cenários os mais particulares existentes – como o da segurança da saúde pública na pandemia (LEAL, 2020, p. 368).

De todo o arcabouço do anteprojeto, um interessante aspecto que é a disciplina das tecnologias de monitoramento utilizadas massivamente no Brasil que, até o momento, não contam com regulamentação. A previsão consta a partir do artigo 42, classificando a atividade como de risco, devendo ser acompanhada do devido relatório de impacto.

Contudo, observa-se que o anteprojeto, em alguma medida, pode se caracterizar bastante limitador a determinadas atividades relacionadas à segurança públi-

ca, considerando a dicção do artigo 43 declarando como “vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial” (ANTEPROJETO, 2018).

Ou seja, há a possibilidade de extinção das técnicas de monitoramento em tempo real para verificação, por exemplo, de pessoas que possuem mandados de prisão penderes, prática corriqueira em grandes capitais brasileiras. De outro lado, há a crítica acerca das influências que essas tecnologias exercem nos indivíduos, as quais concordamos:

Nota-se que pode também existir um impacto para a livre expressão e desenvolvimento da personalidade. A ciência da observação tende a impactar no comportamento livre dos indivíduos, o que leva a que o uso da tecnologia, particularmente em espaços públicos, sem as devidas salvaguardas e garantias, possa ter um efeito inibidor ou resfriador. Essa situação é mais delicada em contextos de manifestações e protestos, uma vez que nesses casos se engaja também a participação cívica e democrática. Portanto, deve existir um cuidado no desenho e na implementação de tecnologias dessa categoria para que haja o uso responsável e de acordo às salvaguardas e garantias necessárias. (LEMOS *et. al*, 2021, p. 5).

Trata-se, assim, de um importante avanço no âmbito das liberdades fundamentais, na medida em que a proteção no uso penal constitui fator para se assegurar a proteção nos meios digitais. Nesse contexto, Stefano Rodotà (2008, p. 18) lembra que “proteção de dados é uma expressão de liberdade e dignidade pessoais”. Se não bem protegidos e amparados, os dados pessoais podem constituir instrumento a prejudicar diversos direitos já assentados em favor do indivíduo. Dessa maneira, necessária se faz uma releitura dos direitos de liberdade à luz do arcabouço protetivo de dados pessoais, fundamento e condição o exercício dos direitos fundamentais na rede. Nesse sentido,

Sinteticamente, pode-se dizer que, por um lado, o respeito ao direito à proteção dos dados pessoais se configura como uma pré-condição para fruição plena dos outros direitos fundamentais; e, por outro lado, impõe uma reconstrução dos direitos fundamentais específicos no novo contexto social delineado pelas tecnologias da informação e da comunicação (RODOTÀ, 2008, p. 200).

Um dos aspectos previstos na Lei Geral de Proteção de Dados e que guarda forte relação com a liberdade é o consentimento. Como visto, trata-se de base legal de suma importância, pois é a partir do consentimento que o titular de dados manifesta concordância com determinada forma de tratamento de dados. Doneda (2019, p. 297) aduz que se trata de manifestação da autonomia da vontade do usuário na forma do tratamento de dados e “compreende um poder conferido à pessoa de modificar sua própria esfera jurídica, com base na expressão de sua vontade” (DONEDA, 2019, p. 298).

Por outro lado, o mesmo autor refere a existência de um mito sobre tal consentimento, tido como caráter meramente acessório e sem muita relevância para o tratamento de dados (DONEDA, 2019, p. 306). Entende-se que esse desafio pode ser superado, inclusive, a partir de uma leitura conjugada com o princípio da finalidade, onde seria vedado o consentimento de forma genérica, certificando-se se o titular possui inteiras condições de entender as consequências de tal instituto (DONEDA, 2019, p. 307).

É importante conferir o destaque para a expressão de liberdade que é o consentimento, a despeito do debate de ampliar a disponibilidade de determinado direito. Bruno Bioni (2021, p. 274-275), em amplo e detalhado estudo sobre o papel do consentimento no tratamento de dados pessoais, afirma que o consentimento não assume a devida importância quando ausentes regulamentações que possibilitem ao cidadão ter conhecimento sobre o uso de suas informações, de forma que as previsões contidas nas políticas de privacidade são insuficientes para tomada de conhecimento de um usuário hipervulnerável.

Nesse sentido, afirma o autor que o consentimento:

*continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a atuação de atores coadjuvantes importantes: i) novas formas para operacionalizá-lo, levando-se em conta a arquitetura (de vulnerabilidade) da rede; ii) o relato normativo complementar da privacidade contextual que o limita e o readapta diante de um solo epistemológico que esfaçela a técnica tradicional da autodeterminação baseada de declaração de vontade do titular dos dados; e iii) o cidadão também exerce um domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com suas legítimas expectativas. Portanto, o conteúdo jurídico-normativo de autodeterminação informacional vai além do consentimento (BIONI, 2021, p. 276).*

Em semelhante afirmativa, Lima acrescenta:

No entanto, a proteção dos dados pessoais não pode ser estruturada tão somente com base no consentimento livre e informado do titular dos dados, em razão de sua vulnerabilidade. Em outras palavras, o indivíduo, que necessita de serviços essenciais na sociedade informacional, quando solicitadas informações que lhe digam respeito para poder usufruir do serviço, não poderá resistir à anuência exigida pelos prestadores de serviços ao tratamento de seus dados pessoais.

Justamente por isso, o consentimento do titular dos dados é insuficiente para a efetiva proteção dos dados pessoais, daí a importância de uma entidade de controle que seja independente para desempenhar sua relevante missão, qual seja a de fiscalizar e garantir o cumprimento da legislação sobre proteção de dados pessoais (LIMA, 2020, p. 124).

Nesse sentido, é possível visualizar o nascedouro de um devido processo informacional, que regulamente medidas legais e procedimentais para a forma com que dados pessoais serão tratados, uma vez que impactam diretamente nas liberdades individuais e coletivas (BIONI *et al.*, 2020, p. 9). Em grande medida, o tratamento de dados pessoais, seja através do consentimento ou de outros mecanismos protetivos, perpassa por procedimentos que podem ser vistos como o devido processo informacional.

Em certa medida, foi omissa a LGPD posto que não trouxe amplas previsões sobre o relatório de impacto no tratamento de dados pessoais, que também, aparentemente, não foi objeto de preocupação do anteprojeto, limitando-se a referir hipóteses de sua necessidade ou possibilidade de requisição do documento. A ausência de diretrizes mínimas que devem estar presentes em documento de tamanha importância no tratamento de dados acarreta a fragilização das formas de operabilidade de tratamento, possibilitando concretos riscos à pessoa. Conforme crítica (BIONI *et al.* 2020, p. 9):

Nesse sentido, um dos pontos criticáveis da Lei Geral de Proteção de Dados foi não indicar procedimentos mínimos para a confecção do relatório de impacto à proteção de dados (uma das espécies de avaliação de impacto que serão tratadas na nota), que hoje é uma das principais ferramentas de governança em diferentes ordenamentos jurídicos. E, mesmo nos casos em que o legislador adotou uma técnica mais prescritiva, como foi o caso Europeu, na GDPR, ainda existem muitas disputas interpretativas sobre como extrair uma normatividade que desencadilhe uma proteção robusta para os titulares dos dados.

Salienta-se que a existência de previsões procedimentais, ainda mais em relação a dados tratados pelo Estado, como no caso da LGPD-Penal, resguardam o devido processo legal e aqui que se tem chamado de devido processo informacional,

pois, assim “garante-se **contraditório e ampla defesa, o que ganha relevo ainda maior na seara penal, uma vez que as decisões ali tomadas impactam** um dos bens jurídicos cuja perda é de maior gravidade: a liberdade de locomoção” (BIONI *et. al.* 2020, p. 9) [grifo do autor]. Ou seja, é preciso ampliar o rol de direitos que tutela a pessoa no ambiente digital, perpassando não apenas pelo direito fundamental à proteção de dados, mas também pela construção do devido processo informacional.

Ademais, é imperioso referir que um devido processo informacional é sustentáculo da separação informacional de poderes, de modo a se alçar a um Estado Democrático Digital de Direito:

É nesse sentido, que — para ilustrar a questão — se revela imperiosa a vedação de bases de dados comuns, cujo compartilhamento é ilimitado entre e para todos os entes estatais. Dito de outro modo, é crucial que se assegure também uma separação/divisão informacional de poderes.

O devido processo informacional e a separação informacional de poderes devem ser compreendidos e concretizados numa perspectiva afinada com o assim designado constitucionalismo digital, implicando, dentre outros aspectos, uma reconfiguração do Estado e do federalismo brasileiro, e, em virtude disso, do papel dos agentes estatais em razão da atualização do rol de direitos fundamentais, sobretudo a partir da promulgação da EC 115, que incluiu o direito à proteção de dados pessoais no catálogo constitucional (SARLET; SARLET, 2022).

Destaca-se que no julgamento da ADI 6387 o Supremo Tribunal Federal já mencionou sobre o devido processo informacional. O Ministro Gilmar Mendes em seu voto ressalta:

É possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro “devido processo informacional” (informational due process privacy right), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos punitivos e peremptórios (BRASIL, 2020).

Logo, há que se balizar que a legislação forneça uma adequada proteção jurídica aos dados pessoais, destinado a também se proteger a liberdade. Veja-se que os impactos no tratamento de dados pessoais possui, inclusive, consequências democráticas, como é o caso célebre da Cambridge Analytica:

O escândalo envolvendo o Facebook e a Cambridge Analytica revela em que medida é possível, em democracia, promover a manipulação do eleitorado socorrendo-se de dados obtidos ilegitimamente (87 milhões de internautas tiveram os seus dados negociados, sem consciência dos visa-

dos, para os efeitos de manipulação eleitoral). Como sabemos, a partir da recolha de informação de 300.000 internautas (através de um inquérito/jogo), o Facebook permitiu a apropriação indevida de dados pessoais de milhões de pessoas. No Reino Unido, tanto quanto se sabe, 1.1 milhão de cidadãos foram alvo de tal apropriação. Ora, se a diferença entre o Remain e o Exit foi de 1.3 milhões de votos, é legítimo presumir que a manipulação levada a efeito pode ter sido determinante nos resultados do referendo britânico.

Não é, pois, um dado adquirido que a revolução tecnológica conduza ao efetivo empoderamento dos cidadãos e ao aperfeiçoamento das instituições democráticas. Os cidadãos podem ser crescentemente marginalizados ou manipulados nos processos de decisão. Não se pretende com isso fragilizar os esforços no sentido do desenvolvimento de uma democracia digital – cujo conceito implica a utilização de meios eletrónicos de comunicação para potenciar e ampliar a ação dos cidadãos e (tendencialmente) controlar os governantes e as instituições públicas. (SILVEIRA; FROUFE, 2018, p. 16)

A figura da Autoridade Nacional de Proteção de Dados Pessoais é importante elemento no resguardo da liberdade e para se resguardar a proteção individual e coletiva, inclusive da própria democracia. Recentemente, por exemplo, a Autoridade Nacional em conjunto com o Tribunal Superior Eleitoral publicaram guia conjunto sobre prevenção e tratamento de dados no período eleitoral. Vale destacar, nessa toada, que dados sobre convicções políticas são considerados dados sensíveis à luz da LGPD, cujo tratamento ganha contornos específicos.

Eis, aqui, um interessante paradoxo de há muito apontado por Rodotà (2008, p. 145):

Se examinarmos a disciplina dos dados “sensíveis”, ao lado daqueles que efetivamente se referem ao direito de ser deixado só (como os relativos à saúde ou à vida sexual) estão os dados referentes às opiniões políticas ou sindicais, à filiação a partidos políticos ou outras associações. Esses últimos dados não se destinam a permanecer reservados ou secretos. Pelo contrário, caracterizam a esfera pública, devem poder ser livremente expostos em público para oferecer a cada um a possibilidade de participar plenamente da vida civil e política. Se a eles é atribuída uma tutela particularmente forte, é para evitar discriminações ou exclusões. O objetivo, portanto, não é o de favorecer a solidão, mas o de garantir a igualdade.

Nesse sentido, a figura do Estado deve reassumir o seu protagonismo na garantia dos direitos fundamentais, uma vez que o “risco à liberdade digital ameaça ‘somente’ algumas das principais conquistas da civilização moderna: liberdade e autonomia pessoais, privacidade e as instituições básicas da democracia e do direito, todas baseadas no Estado-nação” (BECK, 2018, p. 187).

Essa garantia, certamente, deve ser balanceada diante da economia informacional, de modo a não se inviabilizar o desenvolvimento de oportunidades e pes-

quisas baseadas nas operações com tratamento de dados. E, além disso, Beck (2018, p. 188) refere que há a formação de verdadeiro poder central digital autônomo, travestido de uma fachada democrática.

Disso que exsurge a importância da Autoridade Nacional, cujo papel não somente é o de fiscalizar e sancionar, mas de expedir orientações e normativas acerca do tratamento de dados pessoais no Brasil (BRASIL, 2018). Em amplo estudo realizado sobre a atuação de uma autoridade desse tipo, Lima (2020, p. 255) reafirma a necessidade de se conferir a devida independência ao órgão, na medida em que possibilita uma atuação mais marcada para fiscalização de entes públicos e privados.

Contudo, é visível que o poder de fiscalização e controle do órgão possibilitará que o indivíduo que entender lesado em sua liberdade ou em seus dados se socorra da tutela administrativa. Essa possibilidade, inclusive, foi assentada no Protocolo Adicional da Convenção de Estrasburgo, onde se visualizou a necessidade de ampliação dos poderes de investigação e intervenção (LIMA, 2020, p. 259), destacando-se, como antes referido, que os poderes da Autoridade Nacional não apenas assumem o papel legiferante, mas de uma Autoridade judicante e investigativa.

Ora, os danos decorrentes dos riscos e da má gestão no tratamento de dados pessoais são irreversíveis, de modo que o ordenamento deve prever não somente mecanismos, mas instituições capazes de defender e garantir direitos. Ademais, a assertiva de Beck sobre a realidade cosmopolita digital é válida e deve ser levantada ao debate, posto que, diante da economia global, se falar em uma “perspectiva cosmopolita sobre o risco digital abre o horizonte para a ação alternativa” (BECK, 2018, p. 194).

Ressalta-se que na quadra histórica atual, os riscos, mesmo que produzidos em âmbito global, podem se tornar verdadeira ameaça global (BECK, 2011, p. 26), podendo atingir, inclusive, os seus próprios produtores. Veja-se que um dos exemplos mais emblemáticos é o caso Snowden e os escândalos envolvendo o *Wikileaks* cujos danos envolvendo dados e informações impactaram o globo inteiro. Nesse sentido, Beck afirma que “só nos demos conta da catástrofe potencial porque um único trabalhador independente a serviço da CIA aplicou os meios de controle da informação para contar ao mundo sobre o risco digital” (BECK, 2018, p. 185).

De outro lado, diferentemente dos riscos e danos ecológicos, que são visíveis e perceptíveis, o risco à liberdade digital “não se concentra numa catástrofe que

seja física e real no espaço e no tempo, nem resulta dela ou se refere a ela” (BECK, 2018, p. 185). No caso do Brasil, por exemplo, inúmeras foram as situações onde os riscos à liberdade se manifestaram de modo sutil e imperceptível ao cidadão.

Terra e Mulholland (2018, p. 602-603) referem um caso emblemático envolvendo a empresa Decolar.com, onde ela foi condenada pelo Departamento de Proteção e Defesa do Consumidor ao pagamento de multa de R\$ 7.500.000,00 por, abusivamente, fazer diferenciação de preço de locais de hospedagem e negativa de ofertas de vagas de acordo com a localização geográfica do usuário.

Nesse sentido, denota-se que o tratamento indevido de dados pessoais pode afetar a própria liberdade de escolha do usuário e a sua autodeterminação informativa. Trata-se de se balancear de modo adequado a economia digital/informacional com ditames e padrões mínimos para a proteção da liberdade, o que perpassa por uma adequada operação envolvendo dados pessoais.

Veja-se que se falar em liberdade no ambiente digital importa encarar a liberdade sob inúmeras perspectivas que, de uma forma ou de outra, atualmente esbarram na questão do tratamento de dados pessoais. Sempre são válidas as lições de Rodotà (2008, p. 200) no tocante às ligações entre dados pessoais e os direitos de liberdade, quando afirma que se impõe reconstruir a liberdade no ambiente tecnológico, de modo a se atentar às formações sociais virtuais, as garantias de liberdade pessoal (aqui, inclusive, de circulação no interior do ciberespaço)<sup>47</sup> diante da formulação do corpo eletrônico e da liberdade de circulação em decorrência das massivas vigilâncias impostas ao usuário.

A partir disso, o autor italiano afirma que “não se pode postular a indiferença do quadro tradicional dos direitos a este novo ambiente, mantendo inalterados os critérios hermenêuticos pré-tecnológicos” (RODOTÀ, 2008, p. 201). De todo modo, as imbricações estão presentes, tendo-se essa perspectiva ou não. Veja-se, por outro lado, que a proteção de dados pode ser geradora de uma liberdade, tendo em vista que:

os direitos fundamentais como base da proteção de dados não resultam na obrigação de entender as leis sobre o pano de fundo do papel tradicional delas. Além de permitir o desenvolvimento de novos bens juridicamente tutelados, os direitos fundamentais permitem uma compreensão multidimensional das reservas e das regulamentações. As normas jurídicas não só li-

---

<sup>47</sup> Nesse ponto, as percepções sobre publicidade direcionada e segmentação comportamental são necessárias de serem analisadas pelo brilhante estudo de Bioni (2021), aqui já referenciado.

mitam liberdades. Elas também podem, antes de tudo, criar liberdades, torná-las concretas e influenciar suas condições e pré-requisitos sociais. O direito referente à proteção de dados deve estar fundamentado nas diversas funções e diversas formas do direito (ALBERS, 2016, p. 39).

Ademais, essa perspectiva não pode ser visualizada tão somente de uma liberdade e proteção individual. Como acertadamente pontua Albers (2016 p. 42) “a proteção de dados não pode ser garantia unicamente por mecanismos que concedam às pessoas afetadas a proteção individual e mecanismos individuais de reparação. Também é preciso estabelecer mecanismos institucionais de garantia”. Nesse ponto, observa-se acertada a LGPD, em seu artigo 22, quando prevê a possibilidade de tutela jurisdicional coletiva na defesa dos direitos previstos na Lei (BRASIL, 2018). Logo, considerando o direito fundamental, a perspectiva de proteção deve ser ampliada, com a criação de amplos mecanismos não apenas individuais (os quais levam o consentimento e autonomia da vontade individual em conta, como antes referido), mas inclusive de forma coletiva.

Diante disso, denota-se que, na Sociedade de Risco, visualizada a partir da perspectiva da metamorfose digital, uma ampla proteção aos dados pessoais é não somente um resguardo, mas uma verdadeira necessidade. Nesse sentido, visualizar esse direito em ampla perspectiva é passo necessário para alçar o caráter fundamental e de uma verdadeira cidadania eletrônica (RODOTÀ, 2008, p. 145). No mesmo contexto, Marion Albers (2018, p. 38) apresenta:

A proteção de dados baseia-se em uma compreensão multidimensional de direitos fundamentais e exige descrições inteiramente novas dos interesses protegidos: em vez de bens juridicamente tutelados concebidos de modo individualista, a questão tem a ver com posições jurídicas individuais na socialidade ou, em outras palavras, as posições sociais do indivíduo a serem protegidas por direitos fundamentais. O conjunto de interesses e posições protegidos ainda precisa ser elaborado com maior grau de detalhamento e também terá de ser sempre adaptado dinamicamente a novos perigos.

Dessa maneira, a perspectiva cosmopolita do risco digital é importante passo na questão dos dados pessoais (BECK, 2018, p. 194). O oceano de dados produzido em caráter global por diversos indivíduos ao redor do planeta evidencia essa necessidade de se encarar a proteção jurídica mediante instrumentos que possuam efetividade e, sobretudo, visualizar padrões mínimos mundiais de proteção e regulamentação. Nesse sentido, a diretriz de “coletar tudo” (BECK, 2018, p. 193) impõe

uma ampla e fortalecida proteção, haja vista que destitui princípios básicos da liberdade (BECK, 2018, p. 193). Como já pontou Albers (2016, p. 38):

A legislação precisa regulamentar o processamento de dados de modo apropriado e garantir que o tratamento de informações e dados pessoais não ocorra de maneira irrestrita, ilimitada e intransparente, e tem de assegurar que os indivíduos afetados tenham a possibilidade de obter conhecimento suficiente sobre o processamento de dados e informações pessoais e influência suficiente sobre ele. Neste nível, a presença do Estado é imprescindível.

Com isso, a proposta aqui ensaiada é que essa liberdade deve ser reconstituída a partir da proteção de dados e de toda a complexidade que lhe é inerente. Não é à toa que Marion Albers (2016, p. 44) enuncia que esse direito “à proteção de dados é uma área nova e altamente complexa do direito que ainda precisa de um considerável aprofundamento no tocante ao seu assunto, aos interesses protegidos e aos conceitos apropriados para a regulamentação”.

Logo, assumindo o caráter fundamental e estruturante das relações que impactam no mundo on-line e off-line, a proteção de dados estrutura todo um contexto do direito de liberdade, possibilitando a sua adequada fruição e a imposição de limites aos limites desse direito, de modo que evita ou mitiga a intervenção de terceiros, bem como auxilia na tutela da pessoa humana no ambiente digital.

Vale destacar que esses direitos devem ser visualizados à luz das necessidades de proteção da pessoa no ambiente digital, o que muito implica em diferenciar essas categorias de direitos das concepções pré-tecnológicas dos direitos fundamentais. Ou seja, deve-se visualizar o novo com os olhos do novo, de forma que os direitos fundamentais sejam dignos de tutela na seara digital, não servindo apenas como meros direitos acessórios ou que somente são buscados quando violados, servindo, em verdade, como verdadeiros parâmetros para o desenvolvimento das tecnologias da informação.

Essa perspectiva perpassa também pela formulação de políticas públicas que, inclusive, estão previstas na Lei Geral de Proteção de Dados, cuja competência para promoção de conhecimento dessas políticas é da Autoridade Nacional (BRASIL, 2018). Há também a expectativa de formulação de uma Política Nacional de Proteção de Dados Pessoais e da Privacidade, cujas bases ainda não estão assentadas, mas que, aqui se entende, devem ser pautadas de forma democrática e ampla, considerando o impacto democrático que os dados pessoais possuem atual-

mente. Nesse sentido, como já destacado anteriormente, são os dados a nova economia da sociedade atual, impactando mercados e a própria democracia.

Diante disso, a sua proteção por uma Autoridade Nacional, o fortalecimento de padrões normativos sobre as bases legais, nomeadamente o consentimento, e da ampliação do sistema jurídico de proteção de dados pessoais, ampliam a esfera do âmbito de fruição das liberdades no ambiente digital, de modo a se garantir efetiva garantia ao seu âmbito de proteção. Ademais, há a premente necessidade de se proceduralizar a tutela ao adequado tratamento de dados, mediante aquilo que se convencionou chamar de devido processo informacional, que implica na construção de uma regulamentação suficiente e que possa verdadeiramente nortear o tratamento das informações e tutelar as liberdades no ambiente digital, protegendo o usuário dos riscos existentes nesse âmbito.

## CONCLUSÃO

O presente trabalho teve por objetivo verificar em que medida a Lei Geral de Proteção de Dados brasileira, aliada ao direito fundamental à proteção de dados pessoais, pode contribuir à tutela de direitos fundamentais relacionados à pessoa na Sociedade de Riscos e na Era da Informação, muito especialmente em ambientes digitais, com especial enfoque no direito à liberdade.

A hipótese inicial era a de que a proteção de dados pessoais representava nomeadamente no Brasil importante avanço em face das relações que ocorrem no ambiente digital, em especial tendo presente a Sociedade de Riscos em que vivemos, a partir dos princípios norteadores do tratamento de dados, do papel que o consentimento assume, bem como pela criação de uma Autoridade Nacional de Proteção de Dados Pessoais, em suas funções legiferante e judicante.

O primeiro capítulo trabalhou os aspectos coesivos das teorias da Sociedade em Rede e da Sociedade de Risco permitindo uma ampla e detida análise desses modelos teóricos da sociedade. A primeira conclusão possível é a de que as duas teorias possuem, de fato, importantes elementos coesivos, apesar de distintos momentos históricos, sobretudo nas relações entre tecnologia, sociedade e Estado.

Sob o aspecto aqui estudado, constatou-se que, sobretudo diante da metamorfose digital, a proteção de dados assumiu ponto central na evolução da Sociedade em Rede, haja vista a massiva utilização de dados pra predição comportamental, comércio eletrônico, entre outros. Essa formação social veio acompanhada de diversos riscos que, assim como os riscos ambientais, tão bem trazidos por Beck, acarretam riscos à pessoa, nomeadamente em sua liberdade.

Nesse sentido, percebeu-se que tais riscos são, de fato, incontrolláveis e igualmente podem acarretar o chamado efeito bumerangue, na medida em que os seus produtores podem ser atingidos pelos seus efeitos. Essa lógica se amolda perfeitamente ao fenômeno aqui estudado, pois os vazamentos de dados, a vigilância constante, os riscos envolvendo dados pessoais são fatores presentes nessa “nova” Sociedade de Risco digital. Exsurge, então, a necessidade de se falar na reestruturação do Estado e das normas para se proteger o indivíduo nesse ambiente, especialmente diante dos riscos existentes.

Além disso, constatou-se que cada vez mais o desenvolvimento das tecnologias faz conectar a realidade off-line com a online, de forma que há o encurtamento dessa distância pela presença das tecnologias no cotidiano humano, a qual o direito, principalmente os direitos fundamentais, não devem se manter destacados.

Por sua vez, o segundo capítulo evidenciou que, de fato, os direitos fundamentais devem ser reinterpretados com o surgimento e aprimoramento das novas tecnologias, às quais impactam fortemente na realidade humana. A especial ênfase se deve às metamorfoses do direito de liberdade, que tem seu âmbito de proteção defasado diante das ingerências das tecnologias, muitas vezes à burla dos parques regramentos, exigindo-se uma releitura das liberdades, sob o aspecto das liberdades digitais.

Denota-se que é necessária a releitura da liberdade à luz das novas tecnologias, principalmente na formação do corpo eletrônico e de sua tutela. Nesse sentido, evidencia-se a tutela da liberdade em seus mais variados aspectos, seja a liberdade na vida real, mitigada frente ao uso de georreferenciamento, GPS, controles de informações, seja no ambiente digital, considerando a formação do corpo eletrônico e na mitigação de informações à disposição do usuário na rede, especialmente através da segmentação comportamental.

Nesse cenário, constatou-se que buscar o socorro do direito à privacidade em grande medida não se mostra, por si só, suficiente na proteção do indivíduo no espectro societal aqui analisado. A pesquisa evidenciou que, apesar de ser um direito sempre atento às realidades e com grande elasticidade, os conceitos e posições jurídicas atuais lançam a tutela necessária para o novel direito à proteção de dados pessoais. Em verdade, há uma espécie de esgotamento da tutela da privacidade nesse ambiente, de modo que seu âmbito de proteção se mostra reduzido e impossibilitado de tutelar a pessoa no ambiente digital, sobretudo nos panoramas de risco que a envolvem.

O terceiro capítulo tratou de conceituar e contextualizar as bases em que o direito à proteção de dados pessoais se fundamenta, de modo a se afirmar a existência de um sistema jurídico de tutela aos dados pessoais, materializado pelo seu direito fundamental e pelas legislações ordinárias, com especial destaque à Lei Geral de Proteção de Dados Pessoais.

Nesse sentido, observou-se que a referida lei se assenta em concretos

princípios norteadores do tratamento de dados, caracterizando-se como uma verdadeira lei norteadora e central no que tange às relações que envolvam a temática dos dados pessoais. Ao lado do seu direito fundamental, é possível constatar que a proteção de dados pessoais se constitui com o importante direito da Sociedade de Risco no âmbito da Sociedade em Rede, sobretudo quando pautado na defesa das liberdades digitais.

O papel dos princípios, de fato, constitui um grande avanço na defesa das liberdades, pois permite a interpretação do sistema jurídico à realidade concreta, além de, como dito, nortear o tratamento e as operações envolvendo dados pessoais. Além disso, as bases legais, tidas aqui como taxativas, atuam como balizas às operações com dados pessoais, resguardando tanto a proteção ao próprio indivíduo, como assegurando o âmbito de proteção do direito de liberdade.

A função do consentimento, nesse sentido, restou bem tratada na medida em que é, atualmente, a forma de expressão da liberdade no ambiente digital. Apesar das críticas enquanto base legal para tratamento de dados, eis que vem se observando ele como mero caráter acessório ou negocial, o papel que ele assume frente ao mercado digital é de grande relevância.

Nesse sentido, algumas outras possibilidades devem ser assentadas de forma propositiva como resultado das análises aqui realizadas. A primeira delas é visualizar a complexidade que se tem diante dos novos cenários decorrentes de metamorfose digital e compreender o papel fundamental que a proteção de dados tem na defesa das liberdades, do corpo eletrônico e do próprio indivíduo, inclusive como sustentáculo na proteção de diversos outros direitos. Assim, cada vez mais se tem a necessidade de entender essa complexidade sob o viés dos direitos fundamentais e do constitucionalismo digital, ou seja, sob a ótica das novas tecnologias.

Conforme analisado ao longo da pesquisa, as mudanças relacionadas ao contexto digital implicam na descrição e análise inteiramente nova de categorias e conceitos dos direitos fundamentais, como a própria liberdade, a teoria dos direitos fundamentais, ampliando-se o leque de proteção conferido por esses direitos em nosso sistema.

Valorosa parte dessa complexidade se visualiza também na necessidade de políticas públicas relacionadas ao direito fundamental à proteção de dados. Além da própria proteção conferida pela legislação ordinária, é preciso maior esforço

regulativo nesse sentido, englobando-se, inclusive, a tutela penal para os dados pessoais, de forma a se garantir uma ampla e estratégica proteção do indivíduo, especialmente no que tange ao uso de novas tecnologias para política criminal ou segurança pública, a exemplo das câmeras de videomonitoramento.

Ademais, a criação de instrumentos específicos e mais detalhados que a LGPD devem ser trazidos, como a regulação do mercado digital e aspectos relacionados à transferência internacional, por exemplo. Com isso, estar-se-á a concretizar o modelo de correção entre Estados e particulares, na medida em que o Estado fixará as balizas normativas, podendo o particular tutelar ainda mais os direitos em questão.

Importante fator que não foi devidamente trabalhado pela LGPD, é a importância dos relatórios de impactos em relação aos dados pessoais, pois, para além de documentar as formas de tratamento de dados, pode constituir importantes mecanismos de governança e controlabilidade dos dados. Necessário lembrar que se está a se tratar de direitos fundamentais, cujas intervenções somente podem ser concretizadas mediante previsão legal – para fins da presente análise as bases legais, naquilo que vem se nominando como devido processo informacional.

Os relatórios de impacto se caracterizam como instrumento mediador entre o tratamento de dados pessoais e os riscos associados a essas atividades, mas que, atualmente, não dispõem de diretrizes mínimas para tanto. Isso permite que o usuário e também o agente de tratamento tenham conhecimento, mesmo que mínimo, dos riscos pertinentes.

Além disso, vale destacar a importância da atuação da Autoridade Nacional na tutela das liberdades, considerando se tratar da figura estatal específica nas questões envolvendo dados pessoais, especialmente em seu papel judicante e legislante. Afora as questões envolvendo a sua independência, o destaque necessário deve se fazer a sua atuação sancionatória, investigativa e, principalmente, educativa, através de políticas públicas educacionais, promovendo aquilo que se nomina como a cultura de proteção aos dados pessoais.

De outro lado, mostra-se que o panorama da Sociedade de Risco se visualiza também em nível global, principalmente com a transferência internacional de dados, a desterritorialização da Internet, entre outros fatores, que faz surgir a necessidade de uma atuação a nível internacional, com ampliação das possibilidades normativas mediante tratados e acordos internacionais, buscando

uma disciplina semelhante a nível regional e mundial. Aqui, vale relembrar a situação enfrentada na ADC 51, onde os conceitos centrais de soberania são pauta de discussão.

Os danos decorrentes dos riscos erigidos com o ambiente digital são, de fato, irrecuperáveis, considerando o modo como a sociedade se encontra globalizada. Nesse cenário de riscos, constituir elementos normativos na forma de direitos humanos, direitos fundamentais e legislações regulatórias se mostra não apenas importante, mas necessário à defesa das liberdades na atualidade, inclusive atendendo-se ao princípio da dignidade humana. Em um ambiente que cada vez mais se mostra interligado à realidade, é imperioso se visualizar os direitos fundamentais no novo ambiente, objetivando, ao fim, atender à tutela da pessoa.

À guisa de conclusão e de reafirmação das análises aqui dissertadas, a LGPD e o direito fundamental de proteção de dados são importantes elementos da tutela das liberdades no ambiente digital, mas que também possuem desafios, ambos sintetizados a partir das seguintes proposições: (i) necessário se visualizar os direitos fundamentais a partir da complexidade inerente às novas tecnologias, impondo releituras de alguns aspectos, principalmente o âmbito de proteção de alguns direitos; (ii) a importância do Estado e também dos agentes privados na controlabilidade dos riscos associados à Internet, especialmente os riscos que escapam à ordinaryidade; (iii) especial relevância ocupa a ANPD enquanto agência reguladora, bem como de autoridade judicante no aspecto aqui desenvolvido; (iv) carência legislativa no que toca ao relatório de impacto, que concretiza, no entender da presente pesquisa, panoramas mínimos de controle de riscos e de seu conhecimento, conseqüente também do devido processo informacional; (v) desenvolvimento de novas categorias jurídicas e direitos, a exemplo do devido processo informacional, autodeterminação informativa, releitura da privacidade; (vi) surgimento necessário de legislações globalizadas para que se possa tutelar os direitos que mais são afetados pela Internet, com especial relevância o direito geral de liberdade, como aqui estudado; (vii) papel que os princípios regentes do tratamento de dados pessoais e também de suas bases legais como norteadores e parâmetros normativos e hermenêuticos das situações concretas enfrentadas; (viii) ampliação do aspecto regulatório em diversos pontos de relevância social, como o tratamento de dados para fins penais, maior regulação da Internet das Coisas e da inteligência artificial, bem como ao videomonitoramento com reconhecimento facial,

especialmente nos usos penais e político-criminais.

Dessa forma, conclui-se que o panorama teórico aqui utilizado reforça a hipótese da importância do direito fundamental e de uma Lei Geral de Proteção de Dados Pessoais que, contudo, não esgota as possibilidades de proteção aos direitos fundamentais, diante da necessidade de discussão das proposições acima elencadas como forma de ampliar o âmbito de proteção da liberdade e da pessoa na Sociedade de Risco.

Ademais, a proteção de dados pessoais é importante baliza na discussão entre segurança e liberdade na Internet. Com isso, a regulação dos dados pessoais no Brasil constitui o ponto de equilíbrio em face das relações multifacetadas que envolvem o tema liberdade e segurança. Ora, a partir da noção pendular de Baumann, se está a conferir mais segurança no ambiente digital, se está a diminuir a proteção à liberdade e, do contrário, conferindo maior proteção à liberdade, perde-se no aspecto segurança. Percebe-se, do que foi exposto, que tratar sobre o tema proteção de dados – do qual há muito a se avançar no país – é encontrar o ponto de equilíbrio entre esses dois aspectos.

## REFERÊNCIAS

ALBERS, Marion. A complexidade da proteção de dados. *Revista Direitos Fundamentais & Justiça*, a. 10, n. 35, p. 19-45, jul./dez. 2016.

ALLER, Germán. *La Sociedad del Riesgo*. In Co-responsabilidad social, Sociedad del Riesgo y Derecho penal del Enemigo. Montevideo: Carlos Álvarez-Editor, 2006.

ANTEPROJETO DE LEI DE PROTEÇÃO DE DADOS para segurança pública e persecução penal. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-detrabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outrosdocumentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf>. Acesso em: 17 jan. 2022.

ARROYO, César Landa. Derecho fundamental al Internet: contenido esencial. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-22, out./dez. 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8447>. Acesso em: 10 jan. 2022.

ASSANGE, Julian. *et al.* Cypherpunks: liberdade e o futuro da internet. São Paulo: Boitempo Editorial, 2013.

BAGATINI, Júlia. *O espetáculo na sociedade da informação: política pública de Direito dos Danos por risco do desenvolvimento fundamentada no princípio constitucional da solidariedade*. 2018. Tese (Doutorado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2018. Disponível em: <https://repositorio.unisc.br/jspui/bitstream/11624/2416/1/J%c3%balia%20Bagatini.pdf>. Acesso em: 13 mai. 2021.

BAUMAN, Zygmunt. *Globalização: as consequências humanas*. Rio de Janeiro:

Zahar, 1999

BAUMAN, Zygmunt; LYON, David. *Vigilância Líquida*. Rio de Janeiro: Zahar, 2013.

BECK, Ulrich. *A metamorfose do mundo: novos conceitos para uma nova realidade*. Tradução por Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018.

BECK, Ulrich. *Retorno a la Teoría de la Sociedad del Riesgo*. In Boletín de la A.G.E. N.º 30 – 2000, pág.10, <http://age.ieg.csic.es/boletin/30/01.pdf>, Acesso em: 07 jun. 2021

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

BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. *Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Gen Forense, 2021.

BOLESINA, Iuri; GERVASONI, Tássia A. A curiosa tutela do direito à intimidade como “dever de intimidade”. *Civilistica.com*, v. 9, n. 1, p. 1-35, 9 mai. 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/511/385> Acesso em 18 jan. 2022.

BRANDEIS, Louis D.; WARREN, Samuel D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, dec. 15, 1890.

BRANDT, Laís Michele. *O dever de proteção a autodeterminação informativa na sociedade da informação*. 2018. Dissertação (Mestrado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2018. Disponível em: <https://repositorio.unisc.br/jspui/handle/11624/2438>. Acesso em: 13 jan. 2022.

BRASIL, Constituição (1988). *Constituição da República Federativa do Brasil*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/ConstituicaoCompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm). Acesso em: 18 jan. 2022.

BRASIL. [Lei 10.406] *Código Civil Brasileiro de 2002*. Brasília, DF: Presidência da República. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/L10406compilada.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm). Acesso em: 19 jan. 2022

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2014]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/12965.htm). Acesso em: 05 jan. 2021.

BRASIL. Supremo Tribunal Federal. Ação declaratória de constitucionalidade n. 51/

DF. Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação. Requerido: Presidente da República; Congresso Nacional. Relator: Min. Gilmar Mendes. 2017. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>. Acesso em: 19 jan. 2022.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, [2020]. Disponível em: [http://www.planalto.gov.br/CCIVIL\\_03/\\_Ato2019-2022/2020/Mpv/mpv954.htm](http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm). Acesso em: 14 jul. 2022.

BRASIL. Senado Federal. *Proposta de Emenda à Constituição nº 17, de 2019*. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 24 mai. 2022.

BRASIL, Constituição (1988). *Constituição da República Federativa do Brasil*. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/constituicao/ConstituicaoCompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm)>. Acesso em: 18 mai. 2022.

BRASIL. Supremo Tribunal Federal. Julgamento das Medidas Cautelares nas Ações Diretas de Inconstitucionalidade 6387, 6388, 6389, 6390 e 6393. 2020. Disponível em: [https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa\\_inteiro\\_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=ADI%206387&sort=\\_score&sortBy=desc](https://jurisprudencia.stf.jus.br/pages/search?base=acordaos&pesquisa_inteiro_teor=false&sinonimo=true&plural=true&radicais=false&buscaExata=true&page=1&pageSize=10&queryString=ADI%206387&sort=_score&sortBy=desc). Acesso em: 30 de mai. 2022.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 17 mai. 2021.

CANARIS, Claus-Wilhelm. *Direitos fundamentais e direito privado*. 2ª reimp. Coimbra: Almedina, 1937.

CASTELLS, Manuel. *A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade*. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. *A sociedade em rede*. 17. ed. rev. e ampl. São Paulo: Paz e Terra, 2016.

CASTELLS, Manuel. A Sociedade em Rede: Do conhecimento à acção política. In: CASTELLS, Manuel; CARDOSO, Gustavo (Orgs.). *A Sociedade em Rede: do conhecimento à acção política*. Conferência. Belém (Por): Imprensa Nacional, 2005.

CASTELLS, Manuel. *O poder da comunicação*. São Paulo/Rio de Janeiro: Paz e Terra, 2019.

COMPARATO, Fábio Konder. *A afirmação histórica dos direitos humanos*. 12. ed. São Paulo: Saraiva, 2019.

CRESPO, Danilo Leme; RIBEIRO FILHO, Dalmo. A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Privado*, São Paulo, v. 98, p. 161-186, mar./abr. 2019.

DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria Geral dos Direitos Fundamentais*. 6. ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2018.

DIMOULIS, Dimitri; MARTINS, Leonardo. *Teoria Geral dos Direitos Fundamentais*. São Paulo: Revista dos Tribunais, 2007.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*. 2. ed. São Paulo: Thomson Reuters, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. *Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro: da emergência de uma revisão conceitual e da tutela de dados pessoais*. 2008. Disponível em: <[http://www.ambitojuridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=2460](http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460)>. Acesso em: 26 jan. 2022.

FALBO, Ricardo Nery; KELLER, Rene José. Sociedade de risco: avanços e limites da teoria de Ulrich Beck. *Quaestio Juris*, Rio de Janeiro, vol. 08, nº. 03, 2015. pp. 1992-2015. Disponível em: <https://www.e-publicacoes.uerj.br/ojs/index.php/quaestiojuris/article/view/19388/14181>. Acesso em: 27 mai. 2021.

FARINHO, Domingos Soares. *Intimidade da vida privada e media no ciberespaço*. Coimbra: Almedina, 2006.

FERNANDES, José Pedro Teixeira. Da utopia da sociedade em rede à realidade da sociedade de risco. *Análise Social*, Revista do Instituto de Ciências Sociais da Universidade de Lisboa, Lisboa, 207, XLVIII (2.º), 2013, p. 260-286, ISSN Online 2182-2999. Disponível em: [http://analisesocial.ics.ul.pt/documentos/AS\\_207\\_d01.pdf](http://analisesocial.ics.ul.pt/documentos/AS_207_d01.pdf). Acesso em: 29 mai. 2021.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. *Revista de Direito Brasileira*, Florianópolis, v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 29 mai. 2021.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. In: LIMA, Cíntia Rosa Pereira de. *Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*, São Paulo: Thomson Almedina, 2020. p. 123-140.

FORTES, Vinícius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016.

FORTES, Vinícius Borges; BOFF, Salete Oro. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. *Seqüência: Estudos Jurídicos e Políticos*, Florianópolis, v. 35, n. 68, p. 109-128, jun. 2014. ISSN 2177-7055. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/2177-7055.2013v35n68p109>. Acesso em 22 jan. 2022.

FROSINI, Tommaso Edoardo. Nuevas tecnologías y constitucionalismo. *Revista Derecho del Estado*, [S. l.], n. 15, p. 29–44, 2003. Disponível em: <https://revistas.uexternado.edu.co/index.php/derest/article/view/798>. Acesso em: 31 jan. 2022.

GARCIA, Rafael de Deus.; GONTIJO, Rogério Bontempo Cândido . Algoritmos e segurança pública: controle e vigilância no policiamento baseado em dados. *Revista Latino-Americana de Criminologia*, [S. l.], v. 1, n. 1, p. 14–43, 2021. Disponível em: <https://periodicos.unb.br/index.php/relac/article/view/36735>. Acesso em: 21 mai. 2022.

GORCZEWSKI, Clóvis. *Direitos humanos, educação e cidadania: conhecer, educar, praticar*. 2. ed. Santa Cruz do Sul: EDUNISC, 2016.

GUIDI, Guilherme Berti de Campos; REZEK, Francisco. Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos. *Rev. Bras. Polít. Públicas*, Brasília, v. 8, nº 1, 2018 p.276-288.

HARARI, Yuval Noah. *Sapiens: Uma breve história da humanidade*. Porto Alegre: L&PM Editores S. A., 2020.

JESUS, Damásio de; MILAGRE, José Antônio. *Marco Civil da Internet: comentários à Lei n. 12.965 de 23 de abril de 2014*. São Paulo: Saraiva, 2014.

KOHL, Cleize Carmelinda; LEAL, Mônia Clarissa Hennig. Direitos fundamentais e o dever de proteção: uma análise pautada no sistema constitucional e na decisão do caso Damião Ximenes Lopes vs. Brasil na Corte Interamericana de Direitos Humanos. *Espaço Jurídico Journal of Law [EJLL]*, [S. l.], v. 19, n. 1, p. 149–166, 2018. DOI: 10.18593/ejll.v19i1.6490. Disponível em:

<https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/6490>. Acesso em: 21 jan. 2022.

LANDA, César. (2016). Derecho fundamental al Internet. *Primeras Jornadas Nacionales de Derechos Fundamentales*. p. 1-26, 2016. Disponível em: <http://themis.pe/wp/wp-content/uploads/2016/07/Derecho-al-Internet-y-Libertad-de-Expresio%CC%81n.docx>. Acesso em: 20 jan. 2022.

LANDA, César. Contenido esencial del derecho fundamental a internet: teoría y praxis. *Libro homenaje del Área de Derecho Constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú* Landa. Lima: CICAJ, p. 145-173, 2019. Disponível em : <https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/169015/landa.pdf?sequence=1>. Acesso em: 15 jan. 2022.

LEAL, Rogério Gesta. Direito fundamental à proteção de dados em tempos de pandemia: necessárias equações entre segurança pública e privada. *Revista Brasileira de Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 43, p. 357-374, jul./dez., 2020

LEAL, Rogério Gesta. *Perspectivas hermenêuticas dos direitos humanos e fundamentais no Brasil*. Porto Alegre: Livraria do Advogado, 2000.

LEAL, Rogério Gesta. *A Responsabilidade penal do patrimônio ilícito como ferramenta de enfrentamento da criminalidade*. Porto Alegre: FMP, 2017, Disponível em <http://www.fmp.edu.br/servicos/285/publicacoes/>. Acesso em: 13 abr. 2021.

LEAL, Monia Clarissa Hennig; MAAS, Rosana Helena. “*Dever de proteção estatal*”, “*proibição de proteção insuficiente*” e controle jurisdicional de políticas públicas. Rio de Janeiro: Lumen Juris, 2020.

LEMOS, Alessandra *et al.* *Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública*. Rio de Janeiro: Instituto Tecnologia e Sociedade, 2021.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2010.

LIMA, Cíntia Rosa Pereira de. *Autoridade Nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados*. São Paulo: Almedina, 2020.

LIMA, Cíntia Rosa Pereira de; RAMIRO, Lívia Froner Moreno. Direitos do Titular dos Dados Pessoais. In: LIMA, Cíntia Rosa Pereira de. *Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*, São Paulo: Thomson Almedina, 2020. p. 249-277.

LOPES, Ziel Ferreira. Onde habita o Juiz Hérules? Uma aproximação entre teorias da interpretação e questões institucionais. 2020. Tese (Doutorado em Direito) - Universidade do Vale do Rio dos Sinos, São Leopoldo, 2020. Disponível em:

[http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9331/Ziel%20Ferreri%20Lopes\\_.pdf?sequence=1&isAllowed=y](http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9331/Ziel%20Ferreri%20Lopes_.pdf?sequence=1&isAllowed=y). Acesso em: 27 set. 2022.

LUHMANN, Niklas. *Sociologia del Riesgo*. Cidade do México: Universidad Iberoamericana, 2006.

MACHADO, Marta Rodriguez de Assis. *Sociedade do Risco e Direito Penal*. Uma avaliação de novas tendências político-criminais. São Paulo: IBCCRIM, 2005.

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

MARMELSTEIN, George. *Curso de Direitos Fundamentais*. 7a. ed. São Paulo:Atlas. 2014.

MARQUES, Daniel; LEMOS, André. Sensibilidade performativa e privacidade na Internet das Coisas. 5º Simposio Internacional LAVITS | *Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias*. 29 y 30 de noviembre, 01 de diciembre de 2017. Santiago, Chile, p. 10-31. ISSN 2175-9596

MASI, Domenico de. A sociedade pós-industrial. In: MASI, Domenico. *A sociedade pós-industrial*. 4. ed. São Paulo: SENAC, 2003.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. In: LIMA, Cíntia Rosa Pereira de. *Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019*, São Paulo: Thomson Almedina, 2020. p. 141-161.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: <https://seer.imed.edu.br/index.php/revistadedireito/article/view/4103>. Acesso em: 10 jan. 2022. doi:<https://doi.org/10.18256/2238-0604.2020.v16i1.4103>.

MENDES, Gilmar Ferreira. Os Direitos Fundamentais e seus múltiplos significados na ordem constitucional. *Revista Jurídica Virtual*, Brasília, vol. 2, n. 13, jun. 1999. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/1011/995> . Acesso em: 15 jan. 2022.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*, 11. ed. rev. e atual. São Paulo: Saraiva, 2016.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. *Revista de Direito do Consumidor*, São Paulo, v. 130, p. 471-478, jul./ago. 2020.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 106, p. 37-69, jul./ago. 2016.

MOURA, Raíssa; FERRAZ, Lara. Meios de controle à pandemia da Covid-19 e a inviolabilidade da privacidade. Disponível em: <https://content.inloco.com.br>. Acesso em: 8 jun. 2020.

MUMFORD, Lewis, A cultura das cidades, Belo Horizonte: Itatiaia, 1996.

OLIVEIRA, Odete Maria de; CREMONINI, Lademir José. Reflexões sobre a teoria da sociedade em rede de Castells e a teoria da ação comunicativa de Habermas, *Brazilian Journal of Development*, Curitiba, v. 5, n. 6, p. 5160-5184, jun. 2019. ISSN 2525-8761. Disponível em: <https://www.brazilianjournals.com/index.php/BRJD/article/view/1710/1639>. Acesso em: 17 mai. 2021.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*, São Paulo: Thomson Reuters Brasil, 2019. p. 53-83.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. 1948. Disponível em <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 10 jan. 2022

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Convenção Americana de Direitos Humanos ("Pacto de San José de Costa Rica"), 1969. Disponível em: [https://www.cidh.oas.org/basicos/portugues/c.convencao\\_americana.htm](https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm). Acesso em: 10 jan. 2022.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a resignificação da privacidade. *Revista Brasileira de Direito Civil - RBDCivil*, Belo Horizonte, v. 16, p. 35-56, abr./jun. 2018. Disponível em: <https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/230/212>. Acesso em: 25 jan. 2022.

REIS, Jorge Renato. A vinculação dos particulares aos direitos fundamentais nas relações interprivadas: Breves Considerações. In: *Direitos Sociais & Políticas Públicas: Desafios Contemporâneos*. Tomo 5. REIS, Jorge Renato dos; LEAL, Rogério Gesta.(org.) Santa Cruz do Sul:Edunisc. 2005.

RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; GLITZ, Gabriela Pandolfo Coelho. Panorama Geral da Lei Geral de Proteção de Dados Pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de Dados Pessoais europeu. *Revista de Estudos e Pesquisas Avançadas do Terceiro Setor*, Brasília, v. 6, n. 2, p. 340-356, jul./dez. 2019. Disponível em: <https://portalrevistas.ucb.br/index.php/REPATS/article/view/11545/pdf>. Acesso em: 03 jun. 2022.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito UFPR*, Curitiba, v. 53, jun. 2011. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 31 jan. 2022. doi:<http://dx.doi.org/10.5380/rfdupr.v53i0.30768>.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: <http://civilistica.com/o-consentimento-informado-e-a-protecao/>. Acesso em: 20 mai. 2022.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel; *Curso de Direito Constitucional*. 6. ed. São Paulo: Saraiva, 2017.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais. *Direito Público*, [S.l.], v. 17, n. 93, jul. 2020. ISSN 2236-1766. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315>. Acesso em: 02 jun. 2022.

SARLET, Ingo Wolfgang; SARLET, Gabrielle Bezerra Sales. Separação informacional de poderes e devido processo informacional. *Consultor Jurídico*. São Paulo, mai. 2022. Disponível em: [https://www.conjur.com.br/2022-mai-13/direitos-fundamentais-separacao-informacional-poderes-devido-processo-informacional-ordem-juridico-constitucional-brasileira#\\_ftn1](https://www.conjur.com.br/2022-mai-13/direitos-fundamentais-separacao-informacional-poderes-devido-processo-informacional-ordem-juridico-constitucional-brasileira#_ftn1). Acesso em: 03 jun. 2022.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 10 ed. rev. atual. e ampl. Porto Alegre: Livraria do advogado, 2010.

SILVA, Virgílio Afonso. A evolução dos direitos fundamentais. *Revista Latino-Americana de Estudos Constitucionais* 6. p. 541-558, 2005. Disponível em: <https://constituicao.direito.usp.br/wp-content/uploads/2005-RLAEC06-Evolucao.pdf>. Acesso em: 15 jan. 2022.

SILVA, Ana Paula Gonzatti da. Dados de comunicação privada eletrônica, jurisdição e cooperação jurídica internacional: Brasil e Estados Unidos. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 5, n. 2, p. 659-702, mai./ago. 2019. <https://doi.org/10.22197/rbdpp.v5i2.238>

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 40. ed., rev. e atual. São Paulo: Malheiros, 2017.

SILVEIRA, Alessandra; FROUFE, Pedro. *Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos*. UNIO – *EU Law Journal*”, vol. 4, No. 2, julho/2018. Disponível em: <https://doi.org/10.21814/unio.4.2.2>. Acesso em: 5 jun. 2022.

SOMBRA, Thiago Luís Santos. *Direito à privacidade e proteção de dados no*

*ciberespaço: a accountability como fundamento da Lex Privacy*. 2019. Tese (Doutorado em Direito) – Universidade de Brasília, Brasília, 2019. Disponível em: <https://repositorio.unb.br/handle/10482/35752>. Acesso em: 02 jun. 2022.

SOUZA, Liége Alendes de. *As redes sociais virtuais como instrumento de construção do espaço público e persecução da democracia substancial no Brasil: (im)possibilidades contemporâneas*. 2014. Dissertação (Mestrado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2014. Disponível em: [https://www.unisc.br/images/curso-24/dissertacoes/2014/liege\\_alendes\\_de\\_souza.pdf](https://www.unisc.br/images/curso-24/dissertacoes/2014/liege_alendes_de_souza.pdf). Acesso em: 13 mai. 2021.

STRECK, Lenio Luiz. *As interceptações Telefônicas e os Direitos Fundamentais: Constituição, Cidadania, Violência: A lei 9.296/96 e seus reflexos penais e processuais*. Porto Alegre: Livraria do Advogado, 1997.

TERRA, Aline de Miranda Valverde; MULHOLLAND, Caitlin. A utilização econômica de rastreadores e identificadores *on-line* de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*, São Paulo: Thomson Reuters Brasil, 2019. p. 601-619.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*, São Paulo: Thomson Reuters Brasil, 2019. p. 287-322.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. 2000. Disponível em: [https://www.europarl.europa.eu/charter/pdf/text\\_pt.pdf](https://www.europarl.europa.eu/charter/pdf/text_pt.pdf). Acesso em: 20 jan. 2022.

UNIÃO EUROPEIA. Convenção Europeia dos Direitos do Homem. 1950. Disponível em: [https://www.echr.coe.int/documents/convention\\_por.pdf](https://www.echr.coe.int/documents/convention_por.pdf). Acesso em: 20 jan. 2022.

VIANA, Eduardo; MONTENEGRO, Lucas; GLEIZER, Orlando. A esfera protegida dos dados pessoais e as intervenções informacionais do Estado: A dogmática constitucional aplicada ao tratamento de dados na Segurança Pública e no Processo Penal. In: BIONI, Bruno; EILBERG, Daniela Dora; CUNHA, Brenda; SALIBA, Pedro; VERGILI, Gabriela. *Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020.

VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. 2007. 297 f. Dissertação (Mestrado em Direito)-Universidade de Brasília, Brasília, 2007. Disponível em: <https://repositorio.unb.br/handle/10482/3358>. Acesso em: 27 jan. 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.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In: BRUNO, Fernanda. et al. Tecnopólicas da Vigilância: perspectivas da margem*. São Paulo: Boi Tempo, 2018. p. 17-68.