

**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO  
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS  
FACULDADE DE DIREITO**

**A LEI 13.709/2018 E A TUTELA DOS DIREITOS DOS TITULARES DOS DADOS  
PESSOAIS NOS CASOS DE DECISÕES AUTOMATIZADAS**

**VITOR ALCEU DE AZEREDO OLIVEIRA FILHO**

**Rio de Janeiro  
2020/2º semestre**

**VITOR ALCEU DE AZEREDO OLIVEIRA FILHO**

**A LEI 13.709/2018 E A TUTELA DOS DIREITOS DOS TITULARES DOS DADOS  
PESSOAIS NOS CASOS DE DECISÕES AUTOMATIZADAS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação da **Professora Dr.<sup>a</sup> Andréia Fernandes de Almeida.**

**Rio de Janeiro**

**2020/2º semestre**

### CIP - Catalogação na Publicação

O481 Oliveira Filho, Vitor Alceu de Azeredo  
A Lei 13.709/2018 e a tutela dos direitos dos titulares dos dados pessoais nos casos de decisões automatizadas / Vitor Alceu de Azeredo Oliveira Filho. -- Rio de Janeiro, 2020.  
129 f.

Orientadora: Andréia Fernandes de Almeida.  
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2020.

1. Proteção de dados pessoais. 2. Lei 13.709/2018. 3. Autodeterminação informativa. 4. Direitos do titular dos dados. 5. Decisões automatizadas. I. Almeida, Andréia Fernandes de, orient. II. Título.

**VITOR ALCEU DE AZEREDO OLIVEIRA FILHO**

**A LEI 13.709/2018 E A TUTELA DOS DIREITOS DOS TITULARES DOS DADOS  
PESSOAIS NOS CASOS DE DECISÕES AUTOMATIZADAS**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação da **Professora Dr.<sup>a</sup> Andréia Fernandes de Almeida.**

Data da Aprovação: \_\_\_/\_\_\_/\_\_\_\_\_.

Banca Examinadora:

\_\_\_\_\_  
Orientador(a)

\_\_\_\_\_  
Co-orientador(a) (Opcional)

\_\_\_\_\_  
Membro da Banca

\_\_\_\_\_  
Membro da Banca

**Rio de Janeiro**  
**2020/2º semestre**

Dedico este trabalho monográfico à minha esposa, à minha mãe, ao meu pai (*in memoriam*), ao meu padrasto (*in memoriam*) e a todos os meus familiares, amigos e professores que me incentivaram a chegar até aqui.

## **AGRADECIMENTOS**

Agradeço à minha mãe e demais entes queridos e amigos, por estarem sempre do meu lado e por acreditarem em meu potencial.

Agradeço ao meu pai, que já não está mais no plano terreno, por ter sido meu melhor amigo e por ter cultivado em mim, desde pequeno, o amor à sabedoria.

Agradeço à minha esposa, por estar ao meu lado durante períodos fundamentais de encerramentos de ciclos que foram o ensino médio e, agora, a graduação, e por ter me incentivado sempre a seguir em frente, enfrentando comigo todas as dificuldades nessa caminhada.

Agradeço à minha orientadora por ter me acolhido nessa etapa final da graduação, bem como pela paciência, compreensão e admirável dedicação, lançando luzes sobre os rumos da minha pesquisa.

Agradeço a todos os professores da graduação (cada vez mais necessários) que se incumbiram da árdua tarefa de transmitir e debater a complexidade do fenômeno jurídico, tornando acessível um conhecimento que a mim, inicialmente, parecia intangível.

Agradeço aos servidores administrativos da FND e da UFRJ como um todo, pela cordialidade e disposição para me ajudar quando necessitei. Cabe, aqui, uma menção honrosa ao meu padrao, que nos deixou recentemente, pelo fato de ter bem servido a esta Universidade por mais de trinta anos na Biblioteca do CCS, tendo passado seus momentos finais aos cuidados de alunos(as) e (prováveis) ex-alunos(as) que hoje militam junto ao Hospital Universitário (HUCFF), os(as) quais, num passado recente ou remoto, sedimentaram seus conhecimentos na mesma Biblioteca.

Agradeço à Universidade Federal do Rio de Janeiro, por propiciar a mim e a toda a sociedade cursos de reconhecida qualidade, dentre eles o curso de graduação em Direito, o qual agora tenho a alegria de concluir.

*“Uma pessoa cuja identidade é subtraída da sua autonomia e consciência e confiada a procedimentos automáticos, à tecnologia de algoritmos e da computação autônoma (autonomic computing). A pessoa novamente entregue à abstração, desencarnada, reduzida a um fantasma tecnológico? Em face de tudo isso, surge a antropologia do homo dignus, que nos obriga a manter a dimensão humana no centro, sua riqueza, imprevisibilidade e liberdade.”*

*(Stefano Rodotà)*

## RESUMO

O presente trabalho tem como objetivo principal a abordagem dos direitos reconhecidos pelo ordenamento jurídico brasileiro à tutela dos direitos dos titulares dos dados pessoais diante de decisões automatizadas, sob o prisma da Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Estabelece, com apoio em doutrinas e documentos normativos nacionais e estrangeiros, um estudo do tratamento do direito à privacidade desde sua concepção inicial até o desenvolvimento dos direitos à proteção dos dados pessoais e à autodeterminação informativa no contexto da sociedade da informação. Busca-se, num momento intermediário, investigar o enquadramento do direito à proteção de dados pessoais como um direito fundamental à luz da Constituição Federal e dos demais marcos normativos brasileiros. Por último, pretende-se explicitar os riscos advindos do tratamento indevido dos dados pessoais no contexto de decisões automatizadas, identificando-se alguns mecanismos de tutela dos direitos dos titulares dos dados pessoais em situações de violação a direitos e garantias fundamentais.

Palavras-chave: Proteção de dados pessoais. Autodeterminação informativa. Lei nº 13.709/2018. Direitos do titular dos dados. Decisões automatizadas.

## **ABSTRACT**

This final paper aims to address the rights recognized by the Brazilian legal system on the protection of personal data subject rights against automated decision-making from the perspective of Brazilian General Data Protection Law (Law n. 13,709/2018). Based on Brazilian legal literature and its data protection standards (as well as the international ones), it is proposed an analysis on the regulation of the right to privacy from its initial conception until the emergence of the right to personal data protection and informational self-determination in the context of the information society. Furthermore, we seek to investigate the conception of the personal data protection right as a fundamental right according to the Brazilian Federal Constitution approach, in addition to other Brazilian legal frameworks. Finally, the paper intends to clarify the risks arising from improper processing of personal data in the context of automated decision-making, by identifying some mechanisms safeguarding the data subject rights and some judicial remedies against fundamental rights violations.

**Keywords:** Personal data protection. Informational self-determination. Law n° 13,709/2018. Data subject rights. Automated decision-making.

## SUMÁRIO

<b>INTRODUÇÃO .....</b>	<b>11</b>
<b>1 DA PRIVACIDADE À PROTEÇÃO DE DADOS NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO .....</b>	<b>15</b>
1.1 A sociedade da informação .....	15
1.2 A economia da informação: os dados como um ativo .....	19
1.3 Dimensões da privacidade, dados pessoais e autodeterminação informativa.....	23
<b>2 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E DA PERSONALIDADE .....</b>	<b>31</b>
2.1 Constitucionalização do direito civil e a proteção da personalidade .....	31
2.2 Proteção de dados pessoais como direito da personalidade.....	34
2.3 Proteção de dados pessoais como direito fundamental.....	38
<b>3 A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018): FUNDAMENTOS, OBJETIVOS E ENUNCIÇÃO DE DIREITOS .....</b>	<b>47</b>
3.1 Os fundamentos e a necessidade de uma Lei Geral de Proteção de Dados Pessoais no Brasil .....	47
3.1.1 Breve panorama das gerações de leis e dos princípios de proteção dos dados pessoais .....	47
3.1.2 A proteção de dados pessoais no ordenamento jurídico brasileiro.....	51
3.2 Fundamentos, objetivos, alcance, principais conceitos e direitos enunciados pela Lei Geral de Proteção de Dados.....	62
3.3 Vigência dos dispositivos da LGPD .....	73
3.4 A manifestação do Plenário do Supremo Tribunal Federal acerca da temática da proteção dos dados pessoais: o caso da MP n. 954/2020 .....	76
<b>4 MECANISMOS DE TUTELA DOS DIREITOS DOS TITULARES DOS DADOS PESSOAIS DIANTE DAS DECISÕES AUTOMATIZADAS .....</b>	<b>80</b>
4.1 Decisões automatizadas e riscos inerentes ao tratamento de dados pessoais por algoritmos .....	80

4.1.1 <i>Big Data</i> , algoritmos e decisões automatizadas .....	80
4.1.2 Base legal para o tratamento de dados pessoais .....	84
4.1.3 Riscos associados ao tratamento indevido de dados pessoais .....	89
4.2 Sistema remedial previsto pela Lei Geral de Proteção de Dados .....	92
4.3 Mecanismos de prevenção ou de limitação à violação dos direitos fundamentais dos titulares dos dados .....	93
4.4 Mecanismos de repressão à violação de direitos dos titulares por tratamento indevido de dados pessoais.....	104
<b>CONCLUSÃO.....</b>	<b>112</b>
<b>REFERÊNCIAS BIBLIOGRÁFICAS .....</b>	<b>120</b>

## INTRODUÇÃO

A sociedade da informação – termo que faz referência aos grandes avanços e transformações científicas e tecnológicas ocorridos, principalmente, a partir do século XX – tem como característica notória a frequente interação do ser humano com a tecnologia, aqui entendida como os dispositivos eletrônicos conectados à rede mundial de computadores – *Internet*.

O fornecimento dos dados pessoais tem se tornado comum no ambiente virtual, fazendo com que o indivíduo perca o controle sobre suas próprias informações, as quais frequentemente são repassadas a terceiros por questões comerciais, além de receberem os mais diversos tipos de tratamento de dados sem que os usuários estejam cientes disso.

Nesse contexto, verifica-se uma espécie de banalização ou descuido no fornecimento de dados pessoais por parte dos usuários no ambiente virtual, bem como o uso indiscriminado de tais dados pelas empresas e pelos próprios governos.

Dessa forma, abre-se espaço para que entidades privadas e públicas tornem-se capazes de estabelecer rótulos e de traçar padrões de hábitos e de comportamentos dos indivíduos, o que dá ensejo a situações de violação aos direitos fundamentais dos cidadãos, especialmente em se tratando da análise dos dados sensíveis.

No que tange ao arcabouço normativo a respeito da proteção de dados pessoais, faz-se válido destacar o Regulamento Geral de Proteção de Dados da União Europeia – GDPR, o qual serviu de base e de inspiração para a edição do diploma legal brasileiro a respeito da temática.

Anteriormente ao GDPR – que se tornou uma espécie de marco regulatório acerca da proteção de dados para diversos países do mundo, até mesmo para aqueles fora do âmbito da União Europeia –, havia sido editada a Diretiva 95/46/CE do Parlamento Europeu com o intuito de assegurar a livre circulação de dados e a proteção das pessoas titulares de tais dados.

No Brasil, o direito à proteção dos dados pessoais não é previsto expressamente pela Constituição Federal de 1988. O que há é uma tutela jurídica reflexa, a qual se dá a partir da interpretação sistemática dos artigos 1º, inciso III; 3º, incisos I e IV; 5º, X, XII e LXXII.

Na esfera infraconstitucional, nenhum diploma legal brasileiro propôs-se a disciplinar, de modo geral e sistemático, o direito à proteção de dados pessoais, dando-se espaço apenas para regulações específicas sobre direito de acesso à informação e tratamento de dados pessoais num contexto setorizado.

Motivado por essa lacuna no ordenamento jurídico brasileiro e, de igual maneira, pressionado pelo surgimento de frequentes escândalos relativos a vazamento de dados pessoais (fazendo-se menção, apenas a título exemplificativo, do vazamento protagonizado pelo *Facebook* no Caso *Cambridge Analytica*) que afetaram milhões de pessoas em escala mundial (incluindo um número considerável de brasileiros), o Congresso Nacional aprovou a Lei nº 13.709 de 2018, recebendo a alcunha de Lei Geral de Proteção de Dados – LGPD.

A edição da LGPD teve como um de seus propósitos instituir mecanismos para coibir a coleta e o tratamento de dados pessoais de modo ilícito, muitas vezes sem a autorização ou ciência do titular de tais dados.

Um ponto importante a respeito da temática dos dados pessoais é que estes, no contexto atual de sociedade hiperinformatizada, atuam como uma espécie de combustível da economia. É a partir da análise e tratamento de tais dados que os algoritmos conseguem transformá-los em informações que, por um lado, sejam úteis do ponto de vista econômico, mas que, por outro lado, geram consequências prejudiciais aos direitos fundamentais dos usuários.

Assim, a justificativa do presente trabalho reside na atualidade e na importância do assunto relativo ao tratamento de dados pessoais pelas entidades privadas e governamentais e os limites legais e constitucionais que devem ser observados pelas decisões automatizadas que gerem consequências na esfera jurídica do indivíduo titular dos dados objeto de tratamento.

O presente trabalho monográfico dissertará sobre a Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) e a tutela dos direitos dos titulares dos dados nos casos que

envolvam as decisões automatizadas de tratamento de tais dados e que gerem consequências negativas na esfera jurídica do titular, traduzidas na violação a um direito fundamental.

A presente pesquisa tem como objetivo geral verificar em que medida é possível, a partir dos direitos, garantias e procedimentos previstos pela Lei Geral de Proteção de Dados, a tutela dos direitos dos titulares dos dados nas hipóteses de decisões tomadas por meios automatizados violadoras de direitos fundamentais.

Para alcançar o objetivo geral acima explicitado, o presente estudo tem o intuito de: (i) analisar o desenvolvimento e as transformações conceituais do direito à privacidade até a concepção de um direito à proteção de dados pessoais; (ii) investigar o enquadramento do direito à proteção de dados pessoais como um direito fundamental e da personalidade à luz da ordem normativa brasileira; (iii) analisar os fundamentos, objetivos e atribuição de direitos constantes na Lei Geral de Proteção de Dados, explicitando alguns marcos normativos brasileiros sobre proteção de dados pessoais; e (iv) explicitar alguns mecanismos de prevenção, limitação e repressão a violações de direitos fundamentais dos titulares dos dados pessoais em casos que envolvam tratamento potencialmente ilícito de dados por meio de decisões automatizadas a partir da perspectiva da LGPD.

Como método de abordagem, pretende-se realizar uma análise hermenêutica da legislação brasileira e de alguns diplomas normativos estrangeiros, além da doutrina nacional e internacional sobre o tema, analisando brevemente alguns casos concretos para, a partir deles, suscitarem-se reflexões e análises acerca dos limites e possibilidades da aplicação dos princípios, regras e procedimentos previstos pela LGPD para tutelar casos de violação aos direitos dos titulares dos dados pessoais.

O método de procedimento a ser empregado, e que definirá a estrutura do relatório de pesquisa, é a monografia dogmática ou operatória, a ser desenvolvida a partir da pesquisa jurídica instrumental doutrinária e legal, por meio das quais serão estudadas tanto as teorias, teses ou opiniões oriundas de estudiosos que se debruçam sobre o estudo da proteção de dados pessoais e das temáticas a ele relacionadas, quanto a sistematização e interpretação de normas jurídicas que regulam o tema em questão.

Por fim, a técnica de pesquisa a ser adotada é o levantamento. Nesse sentido, serão realizadas investigações por meio da consulta de material bibliográfico (e.g. livros, artigos, revistas, boletins, jornais, portais eletrônicos) e documental (e.g. legislação, relatórios, decisões judiciais, pareceres), a partir dos quais se pretende realizar uma leitura analítica que permita tratar, de modo adequado, o problema de pesquisa em tela.

# 1 DA PRIVACIDADE À PROTEÇÃO DE DADOS NO CONTEXTO DA SOCIEDADE DA INFORMAÇÃO

## 1.1 A sociedade da informação

Ao longo dos séculos, a sociedade passou por diferentes formas de organização social, em que cada arranjo conservava um elemento central que atuava como mola propulsora do desenvolvimento social, econômico e cultural de uma civilização. Tal elemento-chave – fator estruturante da sociedade – serve para a delimitação dos marcos históricos respectivos<sup>1</sup>.

Nesse contexto, por exemplo, a terra e as riquezas oriundas dela eram o elemento central de uma sociedade agrícola. Por seu turno, a sociedade industrial foi erguida pelo advento da eletricidade e das máquinas a vapor, as quais possibilitaram a instituição do modelo de produção fabril. Já na chamada sociedade pós-industrial, os serviços (v.g. assistência médica, educação, seguros, serviços bancários, entretenimento) ocupavam o papel central no desenvolvimento econômico<sup>2</sup>.

A partir das últimas décadas do século XX até os dias atuais, delineou-se uma espécie de economia “informacional, global e em rede”, cujo surgimento se deve à revolução orquestrada no campo da tecnologia da informação, de acordo com Manuel Castells<sup>3</sup>. Para este autor, o emprego dessa tríade de adjetivos teria a seguinte explicação:

[A nova economia] É *informacional* porque a produtividade e a competitividade de unidades ou agentes nessa economia [...] dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É *global* porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É *rede* porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação entre redes empresariais.<sup>4</sup>

---

<sup>1</sup>BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2018, p.33.

<sup>2</sup>*ibidem*.

<sup>3</sup>CASTELLS, M. **A sociedade em rede**: Vol. 1. 8.ª ed. São Paulo: Paz e Terra, 2005, p. 119.

<sup>4</sup>*ibidem*, grifos do autor.

Em sua análise, Castells reconhece que, no decorrer da história, a informação e o conhecimento, *per se*, sempre tiveram sua importância no crescimento da economia. No entanto, no paradigma contemporâneo da sociedade informacional, a própria informação tornou-se o produto na cadeia de produção. De modo mais claro: “os produtos das novas indústrias de tecnologia da informação são dispositivos de processamento de informações ou o próprio processamento das informações”.<sup>5</sup>

Em contraposição a épocas passadas nas quais as informações eram preservadas em pequenas comunidades, difundindo-se pelos familiares, amigos e vizinhos por meio de “fofocas” ou histórias, documentadas ou não, nos dias atuais o modo predominante pelo qual a informação é difundida é por meio da eletricidade, “onde a informação pulsa entre massivos sistemas de registro e bancos de dados”.<sup>6</sup>

Daniel Solove oferece um retrato fidedigno, em sua obra *The Digital Person*, daquilo que se poderia chamar de onipresença e da onipotência das tecnologias de tratamento e processamento dos dados na sociedade contemporânea. O autor destaca que:

Nas últimas décadas tem-se testemunhado uma dramática transformação na maneira em que fazemos compras, transações bancárias e resolvemos nossos afazeres cotidianos – mudanças que vem resultando numa proliferação sem precedentes de registros e dados. Pequenos detalhes que eram capturados em memórias ofuscadas ou fragmentos desbotados de papel agora são para sempre preservadas na mente digital dos computadores, em vastos bancos de dados com férteis campos de dados pessoais [...] A tecnologia digital permite a preservação das minúcias de nossas ações cotidianas, de nossos gostos e antipatias, de quem somos e do que possuímos.  
7

No que tange ao cenário de transição de criação de novas técnicas de manipulação da informação, afigura-se relevante destacar duas grandes mudanças: uma de ordem quantitativa e outra de ordem qualitativa no processamento e tratamento de informações<sup>8</sup>.

A primeira mudança guarda relação com o fato de que as novas tecnologias informáticas possibilitaram um inegável incremento na capacidade de armazenamento de grandes volumes de informações: se em tempos idos era necessário reservar incontáveis espaços físicos e mobílias para a guarda de arquivos em papel, discos de vinil, fitas cassetes,

---

<sup>5</sup>*ibidem*, p. 119-120.

<sup>6</sup>SOLOVE, D. J. **The digital person**: technology and privacy in the information age. New York: New York University Press, 2004, p. 2, tradução nossa.

<sup>7</sup>*ibidem*, p.1, tradução nossa.

<sup>8</sup>BIONI, B. R., *op. cit.*, p. 35-36.

disquetes, CDs etc., hoje basta, por exemplo, um disco rígido (*hard disk*) que cabe na palma de nossa mão com capacidade de um *terabyte*<sup>9</sup>, adquirido a preço relativamente módico, para que seja possível a guarda, por tempo indeterminado, de um volume estratosférico de informações em texto, imagem e vídeo.

A segunda mudança, por seu turno, diz respeito ao salto qualitativo no processamento de informações proporcionado por tais tecnologias, que possibilitou maior eficácia e rapidez no acesso à informação armazenada. No exemplo dado por Bioni, vê-se que:

[...] hoje é muito mais fácil efetuar qualquer pesquisa, sobretudo de ordem acadêmica, por meio dos *softwares* das bibliotecas que filtram a sua busca por autor, título, assunto principal, assuntos secundários e outras categorizações. No passado, cabia ao pesquisador acessar o fichero da biblioteca, que, frequentemente, estava catalogado somente com o nome do autor da obra, para ter acesso ao conteúdo propriamente dito (assunto principal, secundário etc.).<sup>10</sup>

E foi justamente esse estado atual de constantes avanços na área da tecnologia da informação (e a crescente interdependência destes instrumentos com os modelos de desenvolvimento econômico) que motivou Solove a conceber sua tese acerca do “Ser Digital”, o qual seria fruto das “colagens eletrônicas” que perpassam a vida de uma pessoa. A vida seria “capturada em registros” e o Ser Digital seria composto pelas informações a seu respeito que circulariam nas redes mundiais de computadores.<sup>11</sup>

Após essa breve exposição acerca dos elementos básicos característicos da assim chamada sociedade da informação (ou sociedade informacional), revela-se oportuno que certas distinções conceituais sejam feitas.

---

<sup>9</sup>WHAT are bits, bytes, and other units of measure for digital information? **Indiana University**, Bloomington, 18 jan. 2018, tradução nossa. Disponível em: <https://kb.iu.edu/d/ackw>. Acesso em: 26 out. 2019: “Um *bit* é um dígito binário, a menor quantidade de dados em um computador. Um *bit* pode armazenar apenas dois valores: 0 ou 1, correspondente aos valores elétricos “desligado” (*off*) ou “ligado” (*on*), respectivamente. [...] *Bits* geralmente são agregados a um grupo de oito *bits*, que formam um *byte*. Um *byte* contém informação suficiente para armazenar um simples caractere de padrão ASCII como, por exemplo, a letra “h”. Um *kilobyte* (KB) equivale a 1.024 *bytes* [...]. A armazenagem e a memória de um computador é geralmente mensurada em *megabytes* (MB) e *gigabytes* (GB). Um romance de extensão mediana contém aproximadamente um MB de informação. Um MB corresponde a 1.024 *kilobytes* [...]. De maneira semelhante, um GB equivale a 1.024 MB [...]. Um *terabyte* (TB) equivale a 1.024 GB; um TB corresponde mais ou menos ao mesmo volume de informações de todos os livros de uma grande livraria, ou aproximadamente 1.610 CDs [...]”.

<sup>10</sup>BIONI, B. R., *op. cit.*, p. 36.

<sup>11</sup>SOLOVE, D. J., *op. cit.*, p. 2.

Afinal, existe alguma diferença semântica relevante entre dados, informação e conhecimento? A resposta é positiva, mas a literatura a respeito da distinção conceitual entre as expressões acima abarca divergências, bem como questões filosóficas e epistemológicas profundas que não são pertinentes ao presente trabalho monográfico.

É suficiente a menção ao magistério de Setzer, pesquisador da área de Ciência da Computação, de acordo com o qual *dado* é “uma sequência de símbolos quantificados ou quantificáveis”, a *informação* é caracterizada (e não conceituada) como “uma abstração informal (isto é, não pode ser formalizada através de uma teoria lógica ou matemática), que está na mente de alguém, representando algo significativo para essa pessoa”, ao passo que o *conhecimento* é “uma abstração interior, pessoal, de algo que foi experimentado, vivenciado, por alguém”.<sup>12</sup>

A fim de tornar mais evidente a referida distinção, o autor em questão elabora alguns exemplos elucidativos. Segundo Setzer, o texto é um dado, uma vez que as letras que lhe dão forma são símbolos quantificados. Também são dados as fotos, figuras, áudios gravados e vídeos, pois tais elementos podem igualmente ser quantificados. Assim, o dado assume a feição de uma “entidade matemática”, podendo ser descrita por meio de representações formais ou estruturais, o que permite que o dado seja armazenado e processado por um computador.

A informação, como visto anteriormente, não admite, a princípio, uma definição, mas uma mera caracterização, na medida em que “‘algo’, ‘significativo’ e ‘alguém’ não estão bem definidos”. O autor esclarece que a frase “‘Paris é uma cidade fascinante’ é um exemplo de informação – desde que seja lida ou ouvida por alguém, desde que ‘Paris’ signifique para essa pessoa a capital da França [...] e ‘fascinante’ tenha a qualidade usual e intuitiva associada com essa palavra.”<sup>13</sup> Destaca, assim, que a informação não pode ser armazenada por um computador, mas apenas a sua representação em forma de dados.

Acerca dos traços característicos do conhecimento, o pesquisador em tela assevera que este:

---

<sup>12</sup>SETZER, V. W. Dado, Informação, Conhecimento e Competência. **DataGramZero**, v. 0, n. 0, dez. 1999, p. 1-3. Disponível em: [www.brapci.inf.br/index.php/article/download/14562](http://www.brapci.inf.br/index.php/article/download/14562). Acesso em: 27 out. 2019.

<sup>13</sup>*ibidem*.

[...] não pode ser descrito; o que se descreve é a informação. Também não depende apenas de uma interpretação pessoal, como a informação, pois requer uma vivência do objeto do conhecimento. Assim, o conhecimento está no âmbito puramente subjetivo do homem ou do animal. Parte da diferença entre estes reside no fato de um ser humano poder estar consciente de seu próprio conhecimento, sendo capaz de descrevê-lo parcial e conceitualmente em termos de informação, por exemplo, através da frase "eu visitei Paris, logo eu a conheço" (supondo que o leitor ou o ouvinte compreendam essa frase).<sup>14</sup>

Feitas tais considerações acerca da sociedade informacional, seus elementos constitutivos, bem como o esboço conceitual sobre dados, informação e conhecimento, a seguir será explicitado, sinteticamente, o papel dos dados como um ativo no contexto da “economia movida a (ou orientada por) dados” (*data-driven economy*).

## 1.2 A economia da informação: os dados como um ativo

Uma das maiores revistas do mundo sobre assuntos relacionados à economia, a *The Economist*, destacou na manchete de sua edição de 06.05.2017 que o recurso mais valioso do mundo não é mais o petróleo, e sim os dados (“*The world’s most valuable resource is no longer oil, but data*”).<sup>15</sup> Os dados surgem, assim, como uma nova mercadoria altamente lucrativa associada a uma indústria em franco crescimento.

Nesse sentido, a figura abaixo, extraída da matéria supracitada, ilustra essa transformação no cenário econômico mundial, retratando os “gigantes da *internet*” (*internet giants* ou *tech giants*) como os responsáveis pela “extração” (coleta), processamento e circulação do “novo petróleo”, numa analogia entre dois grandes setores econômicos: o petrolífero e o de serviços, publicidade e comércio eletrônicos.

<sup>14</sup>*ibidem*.

<sup>15</sup>REGULATING the internet giants. The world’s most valuable resource is no longer oil, but data. **The Economist**, London, 06 maio 2017. Leaders. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 27 out. 2019.

**Figura 1 – Os gigantes da *internet***



Fonte: *The Economist* (2017)

As companhias ilustradas como *giant techs* – Amazon, Uber, Microsoft, Alphabet (controladora do Google), Facebook, Apple e Tesla – ocupavam, à época da edição da matéria em tela, a posição das empresas mais valiosas do mundo, com lucro anual no patamar das dezenas de bilhões de dólares.<sup>16</sup>

Em razão do papel central assumido pelos dados como insumos do novo arranjo econômico, surgiu a expressão *data-driven economy* justamente para designar a “economia movida a dados”, bem como para evidenciar que “o capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais<sup>17</sup>”.

Nessa linha de raciocínio, Ana Frazão aduz que, numa perspectiva econômica, os “dados importam na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Consequentemente, os dados precisam ser processados para que possam gerar valor”.<sup>18</sup>

Prossegue afirmando, ainda, que o ponto crucial para a extração do máximo potencial da *data-driven economy* reside na qualidade e na profundidade envolvendo o processamento dos dados.

<sup>16</sup>*ibidem*.

<sup>17</sup>SRNICEK, N. *apud* FRAZÃO, A. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei geral de Proteção de Dados. In: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 23-52.

<sup>18</sup>FRAZÃO, A., *op. cit.*, p. 26.

Todavia, a autora faz a ressalva de que esse ciclo de exploração dos dados como um bem economicamente útil (“*data as an asset*”, na linguagem técnica empresarial internacional) tem início com a coleta de dados, que ocorre de forma “cada vez mais maciça e muitas vezes realizada sem o consentimento e até sem a ciência dos titulares desses dados”. Assevera, nesse sentido, que, se “os cidadãos não conseguem saber nem mesmo os dados que são coletados, têm dificuldades ainda maiores para compreender as inúmeras destinações que a eles podem ser dadas e a extensão do impacto destas em suas vidas<sup>19</sup>”.

Como constatação de todo esse cenário em que os dados assumem o papel central do desenvolvimento econômico, revela-se oportuno trazer à luz um artigo publicado por especialistas em negócios da *Internacional Business Machines* (IBM), companhia que, apesar de não figurar atualmente entre aquelas que ocupam o topo da pirâmide, figura entre as empresas de tecnologia com destaque no cenário internacional.

No artigo em questão<sup>20</sup>, fala-se em dados como um ativo no contexto da ascensão da economia da informação com foco na possibilidade de se agregar valor no setor da tecnologia denominado *Internet das Coisas*<sup>21</sup> ou simplesmente *IoT* (*Internet of Things*).

Pela avaliação dos autores, o dado está se tornando um “instrumento-chave para mensurar se uma companhia irá permanecer relevante no decorrer da revolução digital<sup>22</sup>”. Além disso, discorrem sobre a crescente facilidade com que se coletam e se armazenam os dados, os quais são oriundos de diversas fontes, fato que, por sua vez, aumenta o fluxo de dados entre as empresas.

---

<sup>19</sup>*ibidem*.

<sup>20</sup>OPHER, A. *et al.* **The Rise of the Data Economy**: Driving Value through Internet of Things Data Monetization [...]. IBM Global Services, New York, 2016. Disponível em: <https://www.ibm.com/downloads/cas/4JROLDQ7>. Acesso em: 28 out. 2019.

<sup>21</sup>PIRES, P. F. *et al.* Plataformas para a internet das coisas. In: MARTINELLO, M.; ROBEIRO, M. R. N.; ROCHA, A. A. A. R. (Org.) **Minicursos do XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. Porto Alegre: Sociedade Brasileira de Computação, 2015, p. 111. Disponível em: <http://sbrc2015.ufes.br/wp-content/uploads/livro-texto-Minicursos.pdf>. Acesso em: 29 out. 2019: “A Internet das Coisas (do inglês Internet of Things – IoT) [Atzori et al. 2010] é um paradigma que preconiza um mundo de objetos físico embarcados com sensores e atuadores, conectados por redes sem fio e que se comunicam usando a Internet, moldando uma rede de objetos inteligentes capazes de realizar variados processamentos, capturar variáveis ambientais e reagir a estímulos externos. Esses objetos interconectam-se entre si e com outros recursos (físicos ou virtuais) e podem ser controlados através da Internet, permitindo o surgimento de uma miríade de aplicações que poderão se beneficiar dos novos tipos de dados, serviços e operações disponíveis. [...]”.

<sup>22</sup>OPHER, A. *et al.*, *op. cit.*, p. 2, tradução nossa.

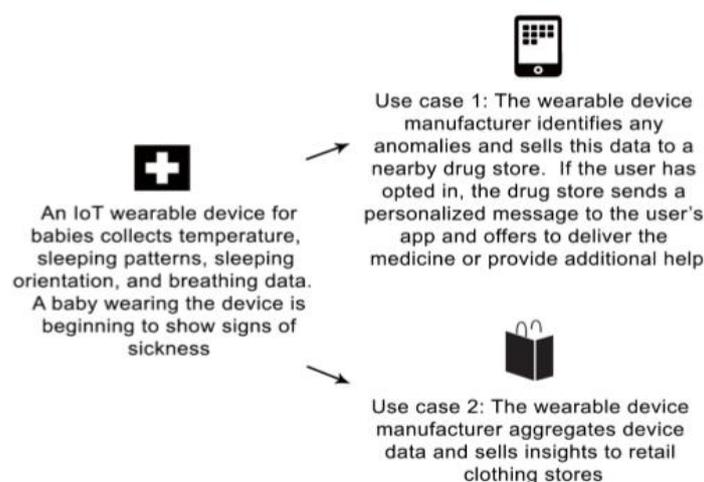
Conforme explicitado pelos especialistas em negócios da IBM:

Dados originários de dispositivos de *IoT* são uma das forças motrizes por trás do salto da economia dos dados. Enquanto um número cada vez maior de “coisas” está se tornando mais instrumentalizado, interconectado e inteligente, o uso dos dados crescerá exponencialmente. Novas abordagens e modelos de negócio serão necessários.<sup>23</sup>

Nessa perspectiva, é importante ressaltar o exemplo dado pelos referidos autores acerca de um possível nicho de monetização de dispositivos que operam pelo mecanismo de *IoT*, coletando e transmitindo dados pela *Internet* em tempo real.

Veja-se:

**Figura 2 – Exemplo de monetização na economia da informação**



Fonte: OPPER *et al.* (2016, p. 2)

Por meio do referido esquema visual, os especialistas em negócios da IBM apresentam ao leitor o exemplo de um dispositivo de *IoT* cuja função é coletar dados de temperatura de bebês, seus padrões e orientações de sono, além de dados sobre respiração. Se, por acaso, um bebê trajando tal dispositivo começa a mostrar sinais de sintomas de alguma doença, haveria a possibilidade de dois “casos de uso” (*use cases*, na linguagem usualmente relacionada à área de Engenharia de *Software*).

<sup>23</sup>*ibidem.*

No primeiro, o fabricante do dispositivo identifica quaisquer anomalias no quadro de saúde do bebê e vende os dados coletados para uma farmácia próxima à sua residência. Se o usuário assim tiver optado, a farmácia enviará uma mensagem personalizada para o usuário do aplicativo e oferecerá a opção de entrega do medicamento adequado ou proverá auxílio adicional. Já no segundo uso de caso, o fabricante reúne dados coletados pelo dispositivo e vende sugestões, baseadas na análise de tais dados, para lojas de roupas infantis.

Percebe-se que a análise da situação retratada anteriormente suscita muitas questões polêmicas e sensíveis relacionadas aos direitos dos usuários de dispositivos dessa natureza. E, com isso, merece atenção o fato de a economia dos dados operar num espaço limítrofe em que, muitas vezes, valores sociais (juridicamente qualificados) como a livre iniciativa e os segredos de negócio entram em rota de colisão com a privacidade e a proteção dos dados pessoais dos titulares em casos semelhantes. Tal problemática será dimensionada, com maior detalhamento, ao longo do presente trabalho.

### 1.3 Dimensões da privacidade, dados pessoais e autodeterminação informativa

Em *Da Privacidade à Proteção de Dados Pessoais*, obra nacional incontornável para aqueles que pretendem imergir na temática da privacidade e suas imbricações com a proteção de dados, Danilo Doneda inaugura o capítulo inicial com a seguinte reflexão:

É característica do nosso tempo a preocupação com questões relacionadas à privacidade e sua tutela. Muitas vezes esta preocupação tem como objeto a busca de um certo isolamento, tranquilidade, refúgio. Outras vezes, não: a busca da privacidade alberga necessidades diversas como a busca da igualdade, da liberdade de escolha, da não discriminação. E, não raro, demonstra estar ligada fortemente à personalidade e ao seu desenvolvimento, em uma complexa teia de relações ainda a serem completamente vislumbradas pelo direito.<sup>24</sup>

A partir dessa breve introdução feita por Doneda, já é possível se antever que a privacidade se caracteriza como um instituto multifacetado, na medida em que seu núcleo conceitual sofreu (e ainda continua a sofrer) diversas modificações de sentido ao longo do tempo.

Em consulta ao dicionário *Michaelis*, a palavra privacidade possui o significado de “[v]ida privada; intimidade, privatividade”. Etimologicamente, indica-se que tal palavra

---

<sup>24</sup>DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p. 7.

deriva da expressão inglesa *privacy* com a junção do sufixo “dade”.<sup>25</sup> Por sua vez, a palavra *privacy*, no *Cambridge Dictionary*, assume o significado de “*the right to be alone and do things without other people seeing or hearing you*”.<sup>26</sup> Ou seja, em tradução livre, seria algo como “o direito de estar só ou direito de ser deixado só e de realizar atividades sem que outras pessoas te vejam ou te escutem”.

Nessa mesma linha, a definição de *privacy* no *Oxford Learner’s Dictionaries* possui dois verbetes, que exprimem o “estado de ficar só e de não ser visto ou perturbado por outrem” e o “estado de estar livre da atenção do público”.<sup>27</sup>

Por último, vale anotar que a palavra de raiz latina *privatus* (derivação de *privo*) assume o significado de “apartado do Estado, peculiar, pessoal, individual, privado”, designando aquilo que é relativo a assuntos pessoais, extraoficiais e das questões alheias ao público.<sup>28</sup>

Verifica-se, desse modo, que as definições acerca da privacidade nos dicionários consultados remetem àquela primeira noção de privacidade apontada por Doneda que denota a “busca de um certo isolamento, tranquilidade, refúgio”, enraizando-se como a concepção presente no senso comum.

Martins aponta que, correntemente, atribui-se essa concepção clássica do “direito a ser deixado em paz” ou do “direito a estar só” ao artigo *The right of privacy* de Samuel Warren e Louis Brandels, publicado em 1890 pela Harvard Law Review (vol. 193). Tal texto é visto como “pioneiro ao estabelecer um marco na doutrina do direito à privacidade, além de certa forma ser profético ao antecipar a importância que a matéria viria a assumir com o desenvolvimento das tecnologias da informação”.<sup>29</sup>

<sup>25</sup>PRIVACIDADE. In: MICHAELIS **Dicionário Brasileiro da Língua Portuguesa**. São Paulo: Editora Melhoramentos, 2015. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=privacidade>. Acesso em: 29 out. 2019.

<sup>26</sup>PRIVACY. In: **CAMBRIDGE Dictionary**. Cambridge: Cambridge University Press, 2019. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/privacy>. Acesso em: 29 out. 2019.

<sup>27</sup>PRIVACY. In: **OXFORD Learner’s Dictionaries**. Oxford: Oxford University Press, 2019, tradução nossa. Disponível em: <https://www.oxfordlearnersdictionaries.com/us/definition/english/privacy?q=privacy>. Acesso em: 29 out. 2019.

<sup>28</sup>PRIVATUS. In: LEWIS, Charlton T. **An Elementary Latin Dictionary**. Nova Iorque: American Book Company, 1890, p. 650, tradução nossa. Disponível em: <https://archive.org/details/anelementarylat01lewigooog/page/n660>. Acesso em: 29 out. 2019.

<sup>29</sup>MARTINS, G. M. O direito ao esquecimento na internet. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.ª ed. Indaiatuba: Editora Foco, 2019, p. 73.

Segundo Doneda, essa noção corrente sobre o que seria privacidade não seria recente, pois “com os sentidos que apresenta, ela pode ser identificada em outras épocas e em outras sociedades”. E, no que tange ao momento da “juridificação” da privacidade, o autor afirma que esta teria passado “a se fazer notar pelo ordenamento jurídico somente no final do século XIX, para assumir suas feições atuais apenas muito recentemente”.<sup>30</sup>

Nesse contexto, o “despertar do direito para a privacidade ocorreu justamente num período em que se mudou a percepção da pessoa humana pelo ordenamento, do qual ela passou a ocupar papel central e ao qual se seguiu a juridificação de vários aspectos do seu cotidiano”.<sup>31</sup>

Na literatura acerca da temática da tutela jurídica dos dados pessoais, é comum a associação destes ao direito à privacidade. Doneda, nesse aspecto, destaca que a proteção dos dados pessoais seria a “continuação por outros meios” da proteção da privacidade, considerando que ambos possuem “pressupostos ontológicos idênticos”.<sup>32</sup>

O autor continua aduzindo que a referida continuidade levada a cabo pelo regime de proteção dos dados pessoais:

[...] assume a tarefa de conduzir uma série de interesses cuja magnitude aumenta consideravelmente na sociedade pós-industrial e acaba, por isso, assumindo uma série de características próprias – especialmente na forma de atuar os interesses que protege, mas também em referências a outros valores e direitos fundamentais. Daí a necessidade de superar a ordem de conceitos pela qual o direito à privacidade era limitado por uma tutela de índole patrimonialista, e de estabelecer novos mecanismos e mesmo institutos para possibilitar a efetiva tutela dos interesses da pessoa. (*idem, ibidem*).

A respeito das atribuições de diferentes sentidos ao conceito da privacidade ao longo da história, destaca-se a análise realizada por Stefano Rodotà<sup>33</sup>, o qual traça “um ponto de chegada na longa evolução do conceito de privacidade, da originária definição – *the right to be let alone* – ao direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada”<sup>34</sup>.

<sup>30</sup>DONEDA, D., *op. cit.*, p. 7-8.

<sup>31</sup>*ibidem*, p. 8.

<sup>32</sup>*ibidem*, p. 27.

<sup>33</sup>RODOTÀ, S. **A vida na sociedade da vigilância**: A privacidade hoje. Rio de Janeiro: Renovar, 2008, *passim*.

<sup>34</sup>MORAES, M. C. B. Apresentação. In: RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 7.

Importa ressaltar, nessa ordem de ideias, que as mudanças nas esferas material e valorativa da sociedade contribuíram sobremaneira para a nova roupagem atribuída ao direito à privacidade.

Em outras palavras, o desenvolvimento das tecnologias da informação (com o advento do fluxo massivo das informações) e o crescente papel central da dignidade da pessoa humana (da qual decorre o princípio do livre desenvolvimento da personalidade) formaram as bases para reconhecer que o tratamento jurídico associado à noção de privacidade como respeito à vida privada e à intimidade já não seria mais suficiente para tutelar os direitos de um indivíduo.

A nova função da privacidade demanda, então, a proteção e a possibilidade de controle dos dados pessoais.

No magistério de Rodotà,

[...] o objeto do direito à privacidade amplia-se, como efeito do enriquecimento da noção técnica da esfera privada, a qual compreende um número sempre crescente de situações juridicamente relevantes. Nessa perspectiva, ao se falar em “privado” não se identificam necessariamente áreas às quais se atribui uma proteção especial por razões de intimidade. Aquela noção tende agora a abranger o conjunto das atividades e situações de uma pessoa que tem um potencial de “comunicação”, verbal e não-verbal, e que pode, portanto, se traduzir em informações. “Privado aqui significa pessoal, e não necessariamente secreto”.<sup>35</sup>

Desse modo, o supracitado autor constata que a estrutura conceitual e funcional do direito à privacidade passa a se concentrar no eixo “pessoa-informação-circulação-controle” no lugar do paradigma clássico da “pessoa-informação-segredo”. Dessa maneira, o “titular do direito à privacidade pode exigir formas de ‘circulação controlada’, e não somente interromper o fluxo das informações que lhe digam respeito”.<sup>36</sup>

Ao referido direito de autonomia sobre o controle das informações dos indivíduos dá-se o nome de *direito à autodeterminação informativa*. Este direito revela-se crucial no âmbito

---

<sup>35</sup>RODOTÀ, S., *op. cit.*, p. 93.

<sup>36</sup>*ibidem*.

das atuais “sociedades da informação”, não havendo dúvidas quanto ao caráter fundamental dos dispositivos normativos que versem sobre tal direito num dado ordenamento jurídico.

A importância do supracitado direito é reforçada pela visão contemporânea de que ““nós somos as nossas informações”, pois elas que nos definem, nos classificam, nos etiquetam; portanto, ter como controlar a circulação das informações e saber quem as usa significa adquirir, concretamente, um poder sobre si mesmo”.<sup>37</sup>

Ainda sobre a tendência interpretativa expansiva da privacidade referida anteriormente, Doneda observa que a privacidade vem a ser dotada de uma dimensão coletiva, estabelecendo-se uma verdadeira ponte entre a tutela da privacidade e o livre desenvolvimento da personalidade. Logo em seguida, dialoga com o pensamento do jurista italiano Stefano Rodotà, ao anotar que este:

(...) observa uma tendência à identificação de sujeitos coletivos, minorias (ou mesmo majorias) de diversas ordens, como entes prejudicados pela violação deste perfil da privacidade, chegando mesmo a afirmar uma tendência à mudança dos sujeitos que demandam pela privacidade, com uma predominância pela coletividade.<sup>38</sup>

Com isso, Doneda conclui que essa roupagem coletiva caracteriza a noção contemporânea da proteção da privacidade, “que se manifesta sobretudo (porém não somente) através da proteção de dados pessoais; e que (...) passa a ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana”.<sup>39</sup>

Sobre tal dimensão coletiva da tutela da privacidade, Pilati e Olivo, no artigo *Direito à privacidade: uma nova perspectiva*, propõem um novo paradigma jurídico que seja capaz de lidar adequadamente com as dimensões assumidas pelo direito à privacidade no contexto da sociedade da informação.<sup>40</sup>

Na visão desses autores, a privacidade ganha contornos coletivos de modo a requisitar formas inovadoras de tutela e de interpretação. Esse novo enquadramento da privacidade

<sup>37</sup>RODOTÀ, S., 1997 *apud* MORAES, M. C. B., *op. cit.*, *loc. cit.*

<sup>38</sup>RODOTÀ, S., 1995 *apud* DONEDA, D., *op. cit.*, p. 30.

<sup>39</sup>DONEDA, D., *op. cit.*, p. 30.

<sup>40</sup>PILATI; J. I.; OLIVO, M. V. C. Direito à privacidade: uma nova perspectiva. **Revista Novos Estudos Jurídicos** (Eletrônica), Itajaí, vol. 19, n. 1, p. 77-94, jan./abr. 2014. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/5543/2948> . Acesso em: 25 out. 2019.

enquanto bem coletivo torna inadequada a sua análise pelas lentes do paradigma jurídico moderno, demandando-se uma “nova moldura interpretativa”, o que só seria possível por meio da teoria jurídica da pós-modernidade.

O conceito de pós-modernidade, por sua vez, decorreria, na ótica de Boaventura de Sousa Santos, de um tipo de “acordo linguístico, embora não muito definido, que a comunidade científica adotou em torno do tema, para caracterizar algo que vem depois da modernidade, superando a sociedade industrial, que por sua vez superou a sociedade agrária”.<sup>41</sup>

Prosseguem afirmando que “o privado já não se circunscreve ao privado tradicional, mas transborda também para o coletivo”. Ressaltam que a análise do bem coletivo a partir dessa nova perspectiva possibilitaria a superação dos

[...] ‘limites estritos dos interesses difusos e a cultura reinante de tutelar o coletivo com instrumentos jurídicos do processo privado tradicional’, [uma vez que] a pós-modernidade, no Direito, não se pauta pelo monismo jurídico, mas pelo pluralismo de fontes, baseando-se nos instrumentos constitucionais, valorizando e redefinindo os procedimentos de tutela para os bens coletivos, em que predomina a dimensão participativa.<sup>42</sup>

Dessa maneira, a sociedade seria concebida como efetiva titular de direitos e, em casos de violações massivas ao direito à privacidade dos cidadãos, a resposta jurisdicional seria mais contundente, eis que o tratamento coletivo a ser conferido ao direito à privacidade permitiria formas mais adequadas de tutela e exercício desse direito.<sup>43</sup>

Após esses breves apontamentos doutrinários acerca do estudo da relação (imbricada) entre privacidade e proteção dos dados pessoais, faz-se válido trazer à evidência o conceito de dados pessoais, os quais podem ser definidos como os dados:

relativos a uma pessoa física ou jurídica, identificada ou identificável, capaz de revelar informações sobre a sua personalidade, relações afetivas, origem étnica ou racial, ou que se refiram às suas características físicas, morais ou emocionais, à sua vida afetiva e familiar, ao domicílio físico e eletrônico, número telefônico, patrimônio, ideologia e opiniões políticas, crenças e convicções religiosas ou filosóficas, estado de saúde físico ou mental, preferências sexuais ou outras análogas que afetem sua intimidade ou sua autodeterminação informativa.<sup>44</sup>

<sup>41</sup>*ibidem*, p. 84.

<sup>42</sup>*ibidem*, p. 83.

<sup>43</sup>*ibidem*, *passim*.

<sup>44</sup>MORAES, M. C. B., *op. cit.*, p. 7.

Frise-se que o conceito acima explicitado teve claras inspirações no que estabelecia a já revogada Diretiva 95/46/CE de 1995 editada pelo Parlamento e Conselho Europeu<sup>45</sup>, em seus artigos 2º e 8º, os quais se referem, respectivamente, aos dados pessoais (sentido comum) e aos dados sensíveis, conforme transcrição abaixo:

Artigo 2º. (Definições). Para efeitos da presente directiva, entende-se por: a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social;

Artigo 8º (Tratamento de certas categorias específicas de dados) 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

Por seu turno, a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018)<sup>46</sup>, em seu artigo 5º, prescreve o conceito de dado pessoal como sendo “informação relacionada a pessoa natural identificada ou identificável” e dado pessoal sensível como aquele “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”.

Todos esses elementos integrantes do conceito de dados pessoais suscitam a reflexão a respeito da possibilidade de se enxergar os dados pessoais como uma espécie de prolongamento da pessoa natural.

Tal concepção é admitida por Danilo Doneda, ao afirmar que em razão “da vinculação intrínseca entre a informação pessoal e a pessoa à qual ela se refere, que é efeito dos dados serem sua representação direta, tal informação deve ser entendida como uma extensão da sua personalidade”.<sup>47</sup>

---

<sup>45</sup>PARLAMENTO EUROPEU E DO CONSELHO. **Diretiva 95/46/CE**, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/eli/dir/1995/46/oj?locale=pt>. Acesso em: 9 jun. 2019.

<sup>46</sup>BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (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: 9 jun. 2019.

<sup>47</sup>BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. (Elaboração: Danilo Doneda). Brasília: SDE/DPDC,

De acordo com Bruno Bioni, para “além da perspectiva subjetiva de que cada ser humano detém seus prolongamentos – atributos e características próprias que o tornam singular –, encaixam-se os dados pessoais como um elemento que compõe essa singularidade”.<sup>48</sup>

O ser humano molda a sua subjetividade a partir das experiências ocorridas no seio social. Sua visão de mundo e o conceito que possui de si e dos outros se originam do incessante fluxo de ideias, conflitos e estímulos exteriores, daí o porquê de se dizer que a “sua singularidade-subjetividade aperfeiçoa-se na social-intersubjetividade”.<sup>49</sup>

Nesse sentido, Bioni é cirúrgico ao abordar a natureza relacional dos direitos da personalidade e, como espécie destes, a proteção dos dados pessoais:

[...] Como bem traçado por Diogo Costa Gonçalves, a pessoa se concretiza quando ela se relaciona (intersubjetividade), isto é, quando ela responde ou procura afirmar quem ela é em meio à comunidade.

A noção completa dos direitos da personalidade liga-se necessariamente à tutela jurídica para que a pessoa possa se realizar e se relacionar junto à sociedade, completando justamente a locução, antes mencionada, projeção social. [...]

Nesse sentido, os dados pessoais não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade). A proteção dos dados pessoais é instrumental para que a pessoa possa livremente desenvolver a sua personalidade<sup>50</sup>

Assim, entendidos como extensão da personalidade, os dados pessoais demandam um tratamento jurídico diferenciado, uma vez que eles se associam a princípios essenciais como o da dignidade da pessoa humana, o livre desenvolvimento da personalidade e demais direitos vinculados ao regime das garantias fundamentais.

Tal perspectiva da proteção de dados como direito fundamental e direito da personalidade será abordada com mais atenção no próximo capítulo.

---

2010, p. 29. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>. Acesso em: 01 set. 2019.

<sup>48</sup>BIONI, B., *op. cit.*, p. 118..

<sup>49</sup>*ibidem*, p. 119.

<sup>50</sup>*ibidem*, p. 118.

## 2 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL E DA PERSONALIDADE

### 2.1 Constitucionalização do direito civil e a proteção da personalidade

Segundo Daniel Sarmiento, a constitucionalização do Direito é um fenômeno que se faz presente na realidade brasileira (assim como em diversos países), operando-se uma quebra do paradigma que alçava os códigos a uma posição privilegiada no ordenamento jurídico e colocava a Constituição em segundo plano, reservando a esta o papel de mera carta de intenções políticas e de documento disciplinador do processo de produção normativa.<sup>51</sup>

As constituições contemporâneas assumem um “papel central no ordenamento jurídico”, pois atuam de maneira a limitar os poderes políticos, incidem diretamente sobre as relações sociais e “seus preceitos e valores são considerados vetores para interpretação e aplicação de todo o Direito, impondo a releitura<sup>52</sup> dos conceitos e institutos existentes nos mais variados ramos do ordenamento”.<sup>53</sup>

Maria Celina Bodin de Moraes observa que o princípio da dignidade da pessoa humana “hoje é reconhecidamente uma conquista determinante e transformação subversiva de toda a ordem jurídica privada”. Em sua visão, o fato de o mencionado princípio ter sido eleito como cláusula basilar da ordem constitucional pátria “alterou radicalmente a estrutura tradicional do direito civil na medida em que determinou o predomínio necessário das situações jurídicas existenciais sobre as relações patrimoniais”.<sup>54</sup>

Nessa mesma trilha, Sarmiento corrobora que essa “nova ótica se traduz [...] nas tendências à personalização e à despatrimonialização deste ramo [Direito Civil] do

---

<sup>51</sup>SARMENTO, D.; SOUZA NETO, C. P. **Direito Constitucional: Teoria, história e métodos de trabalho**. Belo Horizonte: Editora Fórum, 2012, p. 26.

<sup>52</sup>*ibidem*: Sarmiento explicita a distinção entre constitucionalização-inclusão e constitucionalização-releitura. A primeira diz respeito ao “tratamento pela Constituição de temas que antes eram disciplinados pela legislação ordinária ou mesmo ignorados”. A segunda é fruto “de uma consequência da propensão dos princípios constitucionais de projetarem eficácia irradiante, passando a nortear a interpretação da totalidade da ordem jurídica”, de modo que “os preceitos legais, os conceitos e institutos dos mais variados ramos do ordenamento, submetem-se a uma filtragem constitucional, [...] o que muitas vezes impõe significativas mudanças na sua compreensão e em suas aplicações concretas”.

<sup>53</sup>*ibidem*.

<sup>54</sup>MORAES, M. C. B.. A constitucionalização do direito civil e seus efeitos sobre a responsabilidade civil. **Direito, Estado e Sociedade**, Rio de Janeiro, v. 9, n. 29, p. 233-258, jul/dez. 2006, p. 233.

ordenamento”. Isso levaria, sob a ótica principiológica constitucional, ao reconhecimento da “prioridade dos valores existenciais sobre os valores meramente patrimoniais no âmbito jurídico-privado”.<sup>55</sup>

O princípio da dignidade da pessoa humana, conforme sustenta Luís Roberto Barroso: (i) constitui um valor subjacente às democracias constitucionais de modo geral; (ii) funciona “tanto como justificação moral quanto como fundamento jurídico-normativo dos direitos fundamentais”; (iii) por ser parte do núcleo essencial dos direitos fundamentais, assume um papel interpretativo no sentido de “informar a interpretação de tais direitos constitucionais, ajudando a definir o seu sentido nos casos concretos”; (iv) é dotada de eficácia horizontal, pois, “em muitos países, é tida como aplicável tanto às relações entre indivíduos e governo quanto às relações privadas”.<sup>56</sup>

Barroso afirma, ademais, que o conteúdo mínimo do princípio da dignidade humana pressupõe: “1. O valor intrínseco de todos os seres humanos; assim como 2. Autonomia de cada indivíduo; e 3. Limitada por algumas restrições legítimas impostas a ela em nome de valores sociais ou interesses estatais (valor comunitário)”<sup>57</sup>.

Como consequência do novo cenário em que a força normativa da Constituição (terminologia cunhada por Konrad Hesse), assentada no princípio da dignidade da pessoa humana, vincula estruturalmente todo o ordenamento jurídico, a configuração dos direitos da personalidade, como não poderia deixar de ser, passa pela filtragem dos princípios e valores fundantes da Constituição.

De acordo com Gustavo Tepedino, os assim chamados direitos da personalidade pertencem a uma categoria recente de direitos – com raízes nas doutrinas francesa e alemã da segunda metade do século XIX – que abrangem “os direitos atinentes à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade”.<sup>58</sup>

Seguindo essa linha, Sarlet observa que os direitos da personalidade:

---

<sup>55</sup>SARMENTO, D.; SOUZA NETO, C. P., *op. cit.*, p. 28.

<sup>56</sup>BARROSO, L. R. **A dignidade da pessoa humana no direito constitucional contemporâneo**: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Editora Fórum, 2014, p. 64.

<sup>57</sup>BARROSO, L. R., *op. cit.*, p. 72.

<sup>58</sup>TEPEDINO, G.. Premissas metodológicas para a constitucionalização do direito civil. **Revista de Direito do Estado**, Rio de Janeiro, ano 1, n. 2, p. 37-53, 2008, p. 38.

[...] apresentam como aspecto comum o fato de estarem todos vinculados com a proteção da esfera nuclear da personalidade, dignidade e liberdade humanas, o que permite colocar, lado a lado, tantos os direitos à vida e integridade física e psíquica, [...] quanto os demais direitos de caráter pessoal (livre desenvolvimento da personalidade, privacidade, intimidade, honra e imagem, nome etc) [...] <sup>59</sup>

Neste momento inicial de desenvolvimento da natureza e abrangência dos direitos da personalidade, sobrevieram diversas teorias (monistas e pluralistas) dotadas de teor marcadamente patrimonialista, relegando essa nova espécie de direitos a um tratamento jurídico de tipo ressarcitório e dominical. Predominava, portanto, uma visão atrelada ao direito subjetivo à propriedade, a qual sucumbiu em virtude do afloramento de um sistema que concebe a pessoa humana como um fim em si mesmo. <sup>60</sup>

Pela perspectiva da Constituição Cidadã, a personalidade seria concebida “não como um novo reduto do poder do indivíduo, no âmbito do qual seria exercida a sua titularidade, mas como valor máximo do ordenamento, modelador da autonomia privada, capaz de submeter toda a atividade econômica a novos critérios de validade”. Instituiu-se, desse modo, o que se qualifica como “cláusula geral de tutela e promoção da pessoa humana”, sendo esta originária da “escolha da dignidade da pessoa humana como fundamento da República, associada ao objetivo fundamental de erradicação da pobreza e da marginalização, e de redução das desigualdades sociais, juntamente com a previsão do § 2º do art. 5º”. <sup>61</sup>

Moraes ressalta que não há mais lugar para análises herméticas e fracionadas da tutela da personalidade, eis que a leitura mais adequada é aquela que enxerga a sua tutela “de forma unitária, dado o seu fundamento que é a unidade do valor da dignidade da pessoa”. Essa concepção unitária da tutela da personalidade seria ainda mais necessária se for considerado o caráter aberto dos direitos da personalidade, insuscetíveis a uma identificação taxativa, na medida em que a “pessoa humana [...] configura-se como um valor unitário, daí decorrendo o

---

<sup>59</sup>SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D. **Curso de Direito Constitucional**. 8.<sup>a</sup> ed. São Paulo: Saraiva Educação, 2019, p. 559.

<sup>60</sup>TEPEDINO, G. A tutela da personalidade no ordenamento civil-constitucional brasileiro. **Academia**, [2008?], p. 3 e ss. Disponível em: [https://www.academia.edu/31740015/A\\_tutela\\_da\\_personalidade\\_no\\_ordenamento\\_civil-constitucional\\_brasileiro](https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro). Acesso em: 20 jul. 2020.

<sup>61</sup>*ibidem*, p. 23-24.

reconhecimento pelo ordenamento jurídico de uma cláusula geral a consagrar a proteção integral da sua personalidade”.<sup>62</sup>

Os direitos e garantias fundamentais também possuem como base a dignidade da pessoa humana, no entanto, tal categoria não se confunde com a dos direitos da personalidade. Kossmann e Engelmann sintetizam que:

Os direitos de personalidade constituem direitos da própria pessoa humana, portanto, pelo simples fato de sua existência, pelo fato de ser um ser humano; enquanto que os direitos fundamentais, e, portanto, tutelados pela Constituição, visam à proteção do cidadão perante o Estado. “Por isso é que se diz que muitos dos direitos fundamentais são direitos de personalidade, mas nem todos os direitos fundamentais são direitos de personalidade”, podendo esses ser entendidos, portanto, como espécie daqueles, considerando-os como gênero. Miranda ao tratar da distinção entre esses dois direitos, afirma que: “Os direitos fundamentais pressupõem relações de poder, os direitos de personalidade relações de igualdade. Os direitos fundamentais têm uma incidência publicista imediata, quando ocorrem efeitos nas relações entre os particulares; os direitos de personalidade uma incidência privatística, ainda quando sobreposta ou subposta à dos direitos fundamentais...”<sup>63</sup>

Há de se abordar, igualmente, a diferença básica, do ponto de vista da abrangência, entre direitos fundamentais e direitos humanos. Enquanto estes últimos (humanos) são vocacionados à universalização e são historicamente materializados numa compreensão internacional, aqueles (fundamentais) estão inseridos na ordem jurídica dos Estados-nação e são frutos da vontade política-constitucional interna, a partir da qual houve o consenso da necessidade de se conferir um regime jurídico especial a certos direitos.<sup>64</sup>

## 2.2 Proteção de dados pessoais como direito da personalidade

Feita essa pavimentação teórica, cabe agora discorrer sobre o enquadramento do direito à proteção dos dados pessoais como direito da personalidade.

A esta altura, o raciocínio que insere o direito à proteção de dados pessoais na categoria dos direitos da personalidade já se revela intuitivo, na medida em que, conforme já

---

<sup>62</sup>MORAES, M. C. B.. Ampliando os direitos da personalidade. **ResearchGate**, 2010, p. 5-6. Disponível em: [https://www.researchgate.net/publication/288490662\\_Ampliando\\_os\\_direitos\\_da\\_personalidade](https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade). Acesso em: 02 nov. 2019.

<sup>63</sup>KOSMANN, E. L.; ENGELMANN, W. A teoria do fato jurídico e os direitos da personalidade: uma (re)leitura mediada pela Constituição. **Civilistica.com**. Rio de Janeiro, a. 7, n. 3, 2018, p. 8. Disponível em: <http://civilistica.com/a-teoria-do-fato-juridico/>. Acesso em: 04 nov. 2019.

<sup>64</sup>COLAÇO, H. S. **Exercício do direito à autodeterminação informativa nas redes sociais**. 2017. Dissertação (Mestrado em Direito Constitucional) – Fundação Edson Queiroz, Universidade de Fortaleza, Fortaleza, 2017, p. 29.

explicitado no final do capítulo anterior, os dados pessoais de (ou sobre) um indivíduo devem ser considerados como extensão de sua personalidade, pois qualquer espécie de inferência, interferência ou tratamento feito a partir de informações vinculadas a alguém impacta a perspectiva relacional da pessoa, ou seja, quando esta busca responder ou afirmar “quem ela é em meio à comunidade”, o que revela o caráter instrumental da proteção dos dados pessoais para a promoção do livre desenvolvimento da personalidade.<sup>65</sup>

Segundo Kelly Baião e Kalline Gonçalves, no contexto da “sociedade da tecnologia” (também retratada por Manuel Castells como *sociedade informacional* e por Stefano Rodotà como *sociedade da vigilância* e *sociedade da classificação*), o “corpo eletrônico, o conjunto de nossos dados, é objeto de um controle cada vez mais agressivo que precisa ser repensado de acordo com os valores ético-jurídicos a fim de que se possa tutelar aspectos essenciais da personalidade”.<sup>66</sup>

As autoras, retomando as categorias conceituais de Rodotà a respeito do direito à autodeterminação informativa, asseveram que:

O indivíduo só consegue construir de forma livre sua personalidade quando tem consciência da garantia da sua privacidade, esta não mais entendida como o “direito de ser deixado só”, mas como o direito de manter o controle sobre as próprias informações.

A proteção dos dados pessoais torna-se, dessa forma, um valor em si, sintetizando as prerrogativas da pessoa e contribuindo para a nova cidadania (função sociopolítica da privacidade). A privacidade é pré-condição e elemento constitutivo de uma nova forma de cidadania, pois a proteção de dados considerados sensíveis, tais como as opiniões políticas, evita discriminações e permite uma participação mais ampla e igualitária do cidadão na vida pública.<sup>67</sup>

Maria Celina Bodin de Moraes reconhece a característica *não-exaustiva* – também referida como *elástica*, uma vez que abrange um número ilimitado de hipóteses, tendo sempre como norte a cláusula geral de tutela da pessoa humana<sup>68</sup> – dos direitos da personalidade previstos pelo Código Civil brasileiro, não se restringindo apenas aos direitos estipulados

---

<sup>65</sup>BIONI, B. R., *op. cit.*, p. 118.

<sup>66</sup>BAIÃO, K. S.; GONÇALVES, K. C. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 3, n. 2, jul.-dez. 2014, p. 17. Disponível em: <http://civilistica.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-dadignidade-da-pessoa-humana/>. Acesso em: 07 nov. 2019.

<sup>67</sup>*ibidem*, p. 18.

<sup>68</sup>MORAES, M. C. B., 2010, p. 6-7.

pelos artigos 11 a 21 do referido diploma legal,<sup>69</sup> dentre os quais se destacam o direito ao próprio corpo, direito ao nome, direito à honra, direito à imagem e direito à privacidade.

Na análise de Bioni, “um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto, ele deve ser adjetivado como **pessoal**, caracterizando-se como **uma projeção, extensão ou dimensão do seu titular**” [grifo nosso].<sup>70</sup>

O autor avalia, nesse contexto da sociedade informacional e da economia dos dados, que tem se tornado crescente a intensidade da influência das atividades de tratamento de dados na vida das pessoas, que passam a ter aspectos essenciais da vida regulados por tais atividades, uma vez que as esferas social e econômica da civilização “se orientam e movimentam a partir desses signos identificadores do cidadão”. Esses signos representam “um novo tipo de identidade e, por isso mesmo, tais dossiês digitais devem externar informações corretas para que seja fidedignamente projetada a identidade do titular daquelas informações”.<sup>71</sup>

---

<sup>69</sup>BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm). Acesso em: 07 nov. 2019: “[...] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

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

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

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

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

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

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

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

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

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

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

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

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. (Vide ADIN 4815)

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

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

<sup>70</sup>BIONI, B. R., *op. cit.*, p. 99-100.

<sup>71</sup>*ibidem*.

Para Bioni, o direito à proteção de dados pessoais é dotado de autonomia e não deve se restringir à categoria do direito à privacidade, pois o seu bem jurídico (e, pode-se dizer, a sua estrutura e densidade normativa) extrapola a dicotomia tradicional entre público e privado, tendo em vista que a sua construção tem como base o conceito de dado pessoal, o que abre a possibilidade de a informação daí extraída ser de natureza pública ou privada.

Acerca do âmbito da proteção normativa conferida pelo direito à proteção dos dados pessoais, o autor consigna que:

[...] cada vez mais a atividade de tratamento de dados impacta a vida das pessoas, **em particular quando elas são submetidas a processos de decisões automatizadas que irão definir seu próprio futuro.** Nesse contexto, **o direito à proteção de dados pessoais tutela a própria dimensão relacional da pessoa humana,** em especial para que tais decisões não ocasionem práticas discriminatórias, o que extrapola e muito o âmbito da tutela do direito à privacidade. [grifo nosso]<sup>72</sup>

Rodotà, a esse respeito, e tomando por base a mudança paradigmática que põe os interesses existenciais à frente dos interesses patrimoniais, assinala que se sucede um:

[...] profundo processo de revisão dos critérios de classificação das informações pessoais, segundo uma escala de valores renovada, na qual deveria ser garantido o máximo de opacidade às informações suscetíveis de originar práticas discriminatórias e o máximo de transparência àquelas que, referindo-se à esfera econômica dos sujeitos, concorrem para embasar decisões de relevância coletiva.<sup>73</sup>

Já no tocante às reflexões acerca da necessidade de uma tutela diferenciada do direito à proteção de dados pessoais e à autodeterminação informativa, Rodotà constata que:

A presença de **riscos conexos ao uso das informações coletadas,** e não uma natural vocação ao sigilo de certos dados pessoais, foi o que levou ao **reconhecimento de um direito à autodeterminação informativa como direito fundamental do cidadão.** Neste reconhecimento enquadra-se a **tendência de atribuir condições de direitos fundamentais a uma série de posições individuais e coletivas relevantes no âmbito da informação** [...] [grifo nosso]<sup>74</sup>

E é precisamente essa problemática da classificação do direito à proteção de dados pessoais como direito fundamental que será objeto do tópico seguinte.

---

<sup>72</sup>BIONI, B. R., *op. cit.*, p. 127.

<sup>73</sup>RODOTÀ, S., *op. cit.*, p. 35.

<sup>74</sup>*ibidem*, p. 96.

### 2.3 Proteção de dados pessoais como direito fundamental

Após as breves e necessárias reflexões anteriores em torno da lente hermenêutica através da qual deve ser pensado o direito à proteção de dados pessoais, é oportuno, neste momento, lançar luzes sobre o conceito de direitos fundamentais no sistema constitucional brasileiro, analisando se o direito sob análise no presente trabalho (o direito à proteção de dados pessoais e, por arrastamento, o direito à autodeterminação informativa), para além de um direito da personalidade, também se enquadraria, a contento, nessa categoria qualificada pela fundamentalidade em determinado ordenamento jurídico.

Sobre o tema, Ingo Sarlet aduz que, “numa primeira aproximação conceitual, direitos fundamentais são posições jurídicas reconhecidas e protegidas na perspectiva do direito constitucional interno dos Estados”.<sup>75</sup>

Caminhando junto à concepção de José Joaquim Gomes Canotilho, Sarlet sustenta que a fundamentalidade de um direito há de ser avaliada por meio de dois sentidos (ou critérios): o formal e o material.

Sob o ponto de vista formal, a fundamentalidade guarda relação com o fato de determinado direito estar contido, expressa ou implicitamente, na constituição de um país. Além disso, o direito em questão, para que tenha sua fundamentalidade formal reconhecida, precisa estar inserido no seguinte regime normativo: (i) situar-se no topo do ordenamento jurídico, sendo dotado de supremacia hierárquica – qualidade inerente às normas constitucionais; (ii) ser submetido aos limites formais e materiais das hipóteses de reforma constitucional, pressupondo um procedimento especial de alteração legislativa e a eleição de cláusulas substanciais que não podem ser abolidas (cláusulas pétreas – art. 60<sup>76</sup> da

---

<sup>75</sup>SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D., *op. cit.*, p. 411.

<sup>76</sup>BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 13 nov. 2019: “[...] Art. 60. A Constituição poderá ser emendada mediante proposta:

I - de um terço, no mínimo, dos membros da Câmara dos Deputados ou do Senado Federal;

II - do Presidente da República;

III - de mais da metade das Assembléias Legislativas das unidades da Federação, manifestando-se, cada uma delas, pela maioria relativa de seus membros.

§ 1º A Constituição não poderá ser emendada na vigência de intervenção federal, de estado de defesa ou de estado de sítio.

CRFB/1988); (iii) ser diretamente aplicável e vincular de modo imediato as entidades públicas e os atores privados (art. 5º, §1º<sup>77</sup>, da CRFB/1988).<sup>78</sup>

Já a fundamentalidade material requer o exame do conteúdo dos direitos, ou seja, deve-se proceder a uma análise “da circunstância de conterem, ou não, decisões fundamentais sobre a estrutura do Estado e da sociedade, de modo especial, porém, no que diz respeito à posição ocupada pela pessoa humana”.<sup>79</sup> Sarlet ainda observa que a simples investigação a respeito de um direito estar ou não inserido na Constituição Federal pátria é flagrantemente insuficiente, haja vista que o art. 5º, §2º<sup>80</sup>, da CRFB atua como uma cláusula de abertura ao permitir que sejam considerados direitos fundamentais outros direitos que não constem no corpo da Constituição (Título II – Dos direitos e garantias fundamentais).

Atentando-se, ainda, ao sentido material de um direito fundamental, Mendes e Branco lecionam que, a despeito das dificuldades<sup>81</sup> que circundam a tentativa de definir o que se enquadraria ou não no conceito de direito fundamental, o critério norteador seria “a intenção de explicitar o princípio da dignidade da pessoa humana”, aí residindo a “fundamentalidade material dos direitos humanos”.<sup>82</sup> Nessa linha, os referidos autores observam que:

---

§ 2º A proposta será discutida e votada em cada Casa do Congresso Nacional, em dois turnos, considerando-se aprovada se obtiver, em ambos, três quintos dos votos dos respectivos membros.

§ 3º A emenda à Constituição será promulgada pelas Mesas da Câmara dos Deputados e do Senado Federal, com o respectivo número de ordem.

§ 4º Não será objeto de deliberação a proposta de emenda tendente a abolir:

I - a forma federativa de Estado;

II - o voto direto, secreto, universal e periódico;

III - a separação dos Poderes;

IV - os direitos e garantias individuais.

§ 5º A matéria constante de proposta de emenda rejeitada ou havida por prejudicada não pode ser objeto de nova proposta na mesma sessão legislativa. [...]”.

<sup>77</sup>*ibidem*: “[...] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:[...]”

§ 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.[...]”.

<sup>78</sup>SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D., *op. cit.*, p. 412.

<sup>79</sup>*ibidem*, p. 413.

<sup>80</sup>BRASIL, 1988: “[...] § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte [...]”.

<sup>81</sup>Cite-se como exemplo o recorte histórico, isto é, cada momento histórico possuirá um filtro próprio para definir o que seria um direito fundamental. É claro que, se retrocedermos muito na linha do tempo, estaria prejudicada a própria noção de direito fundamental, que é um fenômeno jusfilosófico com raízes na idade moderna. Outro exemplo que ilustra a dificuldade da definição de fundamentalidade material de um direito é o recorte espacial, ou seja, o que hoje se concebe como direito fundamental no Brasil pode não o ser, por exemplo, na Arábia Saudita.

<sup>82</sup>MENDES, G. F.; BRANCO, P. G. G. **Curso de Direito Constitucional**. 13ª ed. rev. e atual. São Paulo: Saraiva Educação, 2018, p. 205.

Não obstante a inevitável subjetividade envolvida nas tentativas de discernir a nota de fundamentalidade em um direito, e embora haja direitos formalmente incluídos na classe dos direitos fundamentais que não apresentam ligação direta e imediata com o **princípio da dignidade humana**, é esse princípio que inspira os típicos direitos fundamentais, atendendo à exigência do respeito à vida, à liberdade, à integridade física e íntima de cada ser humano, ao postulado da igualdade e dignidade de todos os homens e à segurança. [grifo nosso]<sup>83</sup>

José Afonso da Silva, seguindo essa trilha, registra que os direitos fundamentais (os quais denomina de *direitos fundamentais do homem*):

[...] além de referir-se a princípios que resumem a concepção do mundo e informam a ideologia política de cada ordenamento jurídico, é reservada para designar, *no nível do direito positivo*, aquelas prerrogativas e instituições que ele concretiza em garantias de uma **convivência digna, livre e igual de todas as pessoas**. No qualificativo fundamentais acha-se a indicação de que se trata de situações jurídicas sem as quais a pessoa humana não se realiza, não convive e, às vezes, nem mesmo sobrevive [...][grifo nosso]<sup>84</sup>

Outra definição digna de menção é a de Bonavides, segundo o qual:

[c]riar e manter os pressupostos elementares de uma **vida na liberdade e na dignidade, eis aquilo que os direitos fundamentais almejam** [...]. Ao lado dessa acepção lata, que é a que nos serve de imediato no presente contexto, há outra mais restrita, mais específica e mais normativa, a saber: direitos fundamentais são aqueles direitos que o direito vigente qualifica como tais. [grifo nosso]<sup>85</sup>

Nota-se, com isso, que as definições acima comungam de certos elementos. A partir desse pequeno ensaio conceitual, pode-se dizer que para ser alçado à categoria de *fundamental* determinado direito precisa estar conectado, em menor ou maior grau, com a promoção do direito à vida, à liberdade, à igualdade, à integridade física e mental, à segurança e/ou à dignidade da pessoa humana, esta última figurando como fundamento da República Federativa do Brasil (art. 1º<sup>86</sup>, inciso III, da CRFB) e atuando, também, como princípio-

<sup>83</sup>*ibidem*, p. 206.

<sup>84</sup>SILVA, J. A. **Curso de Direito Constitucional Positivo**. 37.<sup>a</sup> ed. rev. e atual. São Paulo: Malheiros Editores, 2014, p. 180.

<sup>85</sup>BONAVIDES, P. **Curso de Direito Constitucional**. 33.<sup>a</sup> ed. São Paulo: Malheiros Editores, 2018, p. 574.

<sup>86</sup> BRASIL, 1988: “[...] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: I - a soberania; II - a cidadania; III - a dignidade da pessoa humana; IV - os valores sociais do trabalho e da livre iniciativa; (Vide Lei nº 13.874, de 2019) V - o pluralismo político.

Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição. [...]”.

matriz que define o filtro a partir da qual todos os outros princípios e regras serão interpretados.

Considerando tudo o que foi abordado até o momento, verifica-se, ao menos numa análise inicial, que o direito à proteção de dados possui *status* de direito fundamental na ordem constitucional brasileira pelas seguintes razões (não exaustivas): (i) tem origem no direito à privacidade (*i.e.*, possuem “pressupostos ontológicos idênticos” na linha do que afirmou Danilo Doneda, como visto no capítulo anterior) e este possui expressa previsão na CRFB, em seu artigo 5º, inciso X<sup>87</sup>; (ii) ainda no âmbito do mencionado art. 5º, há o inciso XII<sup>88</sup>, o qual protege o sigilo das comunicações de dados, previsão esta que, apesar de não se referir diretamente à proteção dos dados e à autodeterminação informativa, já fornece indícios da importância em se assegurar uma tutela na esfera dos fluxos de informação; (iii) no aspecto material, os direitos à proteção dos dados pessoais e à autodeterminação informativa estão vinculados aos ditames da dignidade da pessoa humana, eis que, sendo os dados pessoais uma extensão da personalidade (*i.e.*, da pessoa natural), eventual violação ou tratamento indevido de tais dados resulta no desrespeito à própria dignidade humana e aos princípios dela decorrentes, como o livre desenvolvimento da personalidade; (iv) ainda sob a ótica material, o tratamento indevido ou a utilização dos dados de uma pessoa como base para condutas discriminatórias ou que lesem algum direito fundamental do titular dos dados demonstra que a garantia do direito à proteção de dados pessoais importa na proteção reflexa a outros direitos e garantias fundamentais, como os da igualdade, liberdade, vida digna e desenvolvimento livre da personalidade.

Nessa esteira, a respeito deste último item concernente à proteção reflexa, vale registrar que o ordenamento jurídico brasileiro, em tese, não admite a inadequada proteção dos direitos e garantias fundamentais assegurados aos indivíduos. Isto é: se a Constituição Federal institui uma garantia ou direito fundamental, há de se cuidar para que sejam efetivamente assegurados ao indivíduo o exercício regular de determinado direito e a sua fiel observância e respeito.

---

<sup>87</sup>BRASIL, 1988: “[...] Art. 5º [...] X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;[...]”.

<sup>88</sup>BRASIL, 1988: “[...] Art. 5º [...] 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; (Vide Lei nº 9.296, de 1996) [...]”.

Tal imperativo é extraído da proibição de proteção deficiente (*Untermassverbot*), que, segundo Mendes e Branco, é uma vertente do princípio da proporcionalidade, sendo este amplamente reconhecido pela doutrina brasileira como um princípio constitucional implícito. Estes autores ensinam que:

[...] na dogmática alemã é conhecida a diferenciação entre o princípio da proporcionalidade como proibição de excesso (*Übermassverbot*) e como **proibição de proteção deficiente (*Untermassverbot*)**. No primeiro caso, o princípio da proporcionalidade funciona como parâmetro de aferição da constitucionalidade das intervenções nos direitos fundamentais, como proibições de intervenção. **No segundo, a consideração dos direitos fundamentais, como imperativos de tutela (*Canaris*), imprime ao princípio da proporcionalidade uma estrutura diferenciada. O ato não será adequado quando não proteja o direito fundamental de maneira ótima; não será necessário na hipótese de existirem medidas alternativas que favoreçam ainda mais a realização do direito fundamental; e violará o subprincípio da proporcionalidade em sentido estrito se o grau de satisfação do fim legislativo é inferior ao grau em que não se realiza o direito fundamental de proteção.** [grifo nosso]<sup>89</sup>

Desse modo, um exercício interpretativo possível é aquele que enxerga o direito à proteção dos dados pessoais e à autodeterminação informativa como elementos-chave para garantir a proteção suficiente de outros direitos e garantias que lhes são conexos de algum modo.

Além disso, é importante ressaltar que, apesar de o direito à proteção de dados não constar expressamente e de modo autônomo no catálogo de direitos fundamentais da Constituição Federal, a sua positivação alinha-se ao que ela preceitua em seu artigo 5º, §2º:

Art. 5º [...]

§ 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.

Por consequência, é corrente o entendimento doutrinário reconhecendo que o rol de direitos do artigo 5º é apenas exemplificativo. Admite-se, pois, a existência de direitos fundamentais que não integrem o corpo formal da Constituição. Sobre o tema, Mendes e Branco afirmam que:

É legítimo [...] cogitar de direitos fundamentais previstos expressamente no catálogo da Carta e de direitos materialmente fundamentais que estão fora da lista. Direitos não rotulados expressamente como fundamentais no título próprio da Constituição

<sup>89</sup>MENDES, G. F.; BRANCO, P. G. G., *op. cit.*, p. 750-751.

podem ser assim tidos, a depender da análise do seu objeto e dos princípios adotados pela Constituição. **A sua fundamentalidade decorre da sua referência a posições jurídicas ligadas ao valor da dignidade humana; em vista da sua importância, não podem ser deixados à disponibilidade do legislador ordinário.** (grifo nosso)

Não nos é dado esquecer, ainda, que os direitos são frutos de seu tempo, isto é, são constituídos de maneira histórica e orgânica, atendendo aos reclamos da sociedade. Dissertando sobre a característica histórica dos direitos fundamentais, Norberto Bobbio assevera que:

[...] os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas.<sup>90</sup>

A partir disso, pode-se dizer que o nascimento de um direito fundamental seria ditado pelas “condições ideais de temperatura e pressão” (numa analogia própria da área das ciências naturais) num determinado recorte geográfico e temporal, bem como considerando as peculiaridades sociais, econômicas e políticas de cada sociedade.

Nas palavras de Bobbio, os direitos fundamentais:

**Nascem quando devem ou podem nascer.** Nascem quando o aumento do poder do homem sobre o homem — que **acompanha inevitavelmente o progresso técnico**, isto é, **o progresso da capacidade do homem de dominar a natureza e os outros homens — ou cria novas ameaças à liberdade do indivíduo** ou permite novos remédios para as suas indigências: ameaças que são enfrentadas através de demandas de limitações do poder; remédios que são providenciados através da exigência de que o mesmo poder intervenha de modo protetor. [grifo nosso]<sup>91</sup>

Não há dúvidas de que a atual conjuntura nacional e internacional demanda o reconhecimento do direito à proteção de dados como direito fundamental. Para confirmar a veracidade de tal constatação, basta mencionar que tramita, desde 2019, uma Proposta de Emenda à Constituição (PEC) no Congresso Nacional que tem o objetivo de inserir, formalmente, o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais da Constituição da República Federativa do Brasil.

A proposta em questão é a PEC nº 17/2019, cuja ementa é a seguinte: “Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a

<sup>90</sup>BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004, p. 9.

<sup>91</sup>*ibidem*.

proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria”<sup>92</sup>. Na explicação da ementa consta que a aludida PEC visa a assegurar “o direito à proteção de dados pessoais, inclusive nos meios digitais”, e insere “entre as competências da União legislar sobre a proteção e tratamento de dados pessoais”.<sup>93</sup>

O Senador Eduardo Gomes (MDB-TO) elaborou a justificação da proposta que teve início no Senado Federal e, tendo em vista a sua pertinência em relação aos assuntos até aqui tratados, afigura-se oportuna a menção de alguns trechos que abaixo seguem transcritos:

A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão.

O avanço da tecnologia, por m lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados. [...]

De fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas **já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado.** [...] [grifo nosso]<sup>94</sup>

Após aprovação do texto da PEC 17/2019 no Senado Federal, a referida proposta foi encaminhada para a Câmara dos Deputados (CD), tendo sido recebida pela Mesa Diretora desta casa legislativa no dia 03.07.2019<sup>95</sup>.

Com isso, a aludida PEC encontra-se atualmente em trâmite na Câmara dos Deputados, afigurando-se importante fazer menção ao fato de que, em 10/12/2019, foi apresentada a

<sup>92</sup>BRASIL. **Proposta de Emenda Constitucional 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. Brasília, DF: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 14 nov. 2019.

<sup>93</sup>*ibidem*.

<sup>94</sup>*Ibidem*. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1571776979155&disposition=inline>. Acesso em: 14 nov. 2019.

<sup>95</sup>BRASIL. **Proposta de Emenda Constitucional nº 17, de 2019**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Câmara dos Deputados, 2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 20 jul. 2020.

proposta de um texto substituto elaborado pelo Deputado Orlando Silva (PCdoB-SP), a seguir transcrito:

Art. 1º O art. 5º da Constituição Federal passa a vigorar acrescido com o seguinte inciso:

“Art.5º.....

.....  
LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;  
.....” (NR)

Art. 2º O art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI:

“Art. 21. ....

.....  
XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei, que disporá sobre a criação de um órgão regulador independente.” (NR)

Art. 3º O art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

“Art. 22.....

.....  
XXX – proteção e tratamento de dados pessoais.  
.....” (NR)

Art. 4º Para os efeitos do inciso XXVI do art. 21, na redação dada pelo art. 2º desta Emenda, o órgão regulador será entidade independente, integrante da administração pública federal indireta, submetida a regime autárquico especial.

Art. 5º Esta Emenda Constitucional entra em vigor na data de sua publicação.<sup>96</sup>

Tal texto substitutivo, que foi aprovado, também no dia 10/12/2019 pela Comissão Especial sobre Dados Pessoais, aguarda, desde a referida data, deliberação no Plenário da Câmara dos Deputados.<sup>97</sup>

Neste ponto, é possível notar que o texto substitutivo da PEC pretende oferecer ao direito à proteção dos dados pessoais um tratamento jurídico-constitucional *autônomo* em relação ao direito à inviolabilidade das comunicações de dados (diversamente do concebido no texto original da proposta de emenda em questão).

<sup>96</sup>*ibidem*.

Disponível

em:

[https://www.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1844581&filename=SBT-A+1+PEC01719+%3D%3E+PEC+17/2019](https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1844581&filename=SBT-A+1+PEC01719+%3D%3E+PEC+17/2019). Acesso em: 20 jul. 2020.

<sup>97</sup>*ibidem*.

De qualquer maneira, é pertinente sublinhar que o enquadramento do direito à proteção de dados pessoais no rol expresso de direitos fundamentais da Lei Maior brasileira teria a mera intenção de tirar qualquer espécie de dúvida sobre o caráter fundamental de tal direito. Com base no que se expôs anteriormente, percebe-se que a nota dessa fundamentalidade já existe em seu sentido *material*.

O que se pretende com a PEC nº 17/2019 é apenas reconhecer, do ponto de vista *formal*, o teor fundamental do direito à proteção dos dados (o que, sem dúvidas, aumenta a sua densidade normativa), além de, oportunamente, lidar com a questão da competência legislativa de assuntos dessa natureza, a qual incumbiria à União Federal, por se tratar, justamente, de uma temática vinculada a interesses mais abrangentes – que ultrapassam os interesses local e regional – e que se atrelam, inclusive, a assuntos ligados à segurança nacional.

Feitas essas considerações acerca da caracterização do direito à proteção de dados pessoais como direito da personalidade e direito fundamental à luz do ordenamento jurídico civil-constitucional brasileiro, o capítulo a seguir será dedicado a uma análise mais detida da Lei Geral de Proteção de Dados.

### **3 A LEI GERAL DE PROTEÇÃO DE DADOS – LGPD (LEI Nº 13.709, DE 14 DE AGOSTO DE 2018): FUNDAMENTOS, OBJETIVOS E ENUNCIÇÃO DE DIREITOS**

#### 3.1 Os fundamentos e a necessidade de uma Lei Geral de Proteção de Dados Pessoais no Brasil

##### 3.1.1 Breve panorama das gerações de leis e dos princípios de proteção dos dados pessoais

De acordo com Danilo Doneda, o reconhecimento da autonomia do direito à proteção de dados pessoais – e a consequente previsão de mecanismos de tutela específicos – vem se fazendo presente em muitos ordenamentos jurídicos ao longo das últimas décadas. Destaca o autor que as consequências decorrentes do tratamento automatizado de informações pessoais não apenas justificam alterações pontuais no ordenamento jurídico, mas também, na linha do que foi exposto no capítulo anterior, “formam as bases daquele que vem sendo tratado como um direito fundamental à proteção de dados” num contexto em que “a proteção da pessoa na Sociedade da Informação passava, cada vez mais, a depender diretamente do controle destas sobre seus próprios dados pessoais”.<sup>98</sup>

Doneda, em seu artigo intitulado *O direito fundamental à proteção de dados pessoais*, aborda a temática do desenvolvimento das leis de proteção de dados. Tomando por base a classificação da evolução das leis de proteção de dados pessoais feita por Viktor Mayer-Schonberger, Doneda apresenta as quatro gerações de leis gestadas nas últimas quatro décadas (aproximadamente), abordando os fundamentos, o contexto e as características de cada um delas, as quais:

[...] partem desde uma primeira geração, cujo enfoque era mais técnico e restrito aos grandes computadores de sua época, até a abertura mais recente a técnicas mais amplas e condizentes com a capilaridade e sofisticação das tecnologias adotadas para o tratamento de dados.<sup>99</sup>

A *primeira geração* de leis constituía-se de “normas que refletiam o estado da tecnologia e a visão do jurista nos primórdios da utilização de computadores para o processamento de informações pessoais”. Seu propósito era instituir um marco regulatório

---

<sup>98</sup>DONEDA, D. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.<sup>a</sup> ed. Indaiatuba: Editora Foco, 2019, p. 40.

<sup>99</sup>*ibidem*.

aplicável aos grandes centros de tratamento de dados, aos quais incumbiam a coleta e a gestão dos dados pessoais.<sup>100</sup>

A “gramática” de tais leis focava-se não tanto na questão da tutela da privacidade, mas sim na abordagem técnica de questões relativas aos bancos de dados, aos regimes de autorização e às modalidades de tratamento de dados, citando-se como exemplos “leis que [...] tratavam da concessão de autorização para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos”, bem como regulavam o controle do uso de informações pessoais pela Administração Pública. Tal geração teve como marco final aproximado a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, datada de 1977.

Após a crescente inadequação das leis até então vigentes à nova realidade tecnológica que afluía – “diante da multiplicação dos centros de processamento de dados, que inviabilizou o controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento” – abriu-se espaços para a *segunda geração* de leis de proteção de dados. O traço distintivo dessa geração, surgida no final da década de 1970, era o fato de sua estrutura não estar mais centrada no fenômeno computacional em si, mas na tutela da privacidade e da proteção dos dados pessoais como uma “liberdade negativa, a ser exercida pelo próprio cidadão”, a exemplo da lei francesa de proteção de dados pessoais de 1978 (*Informatique et Libertés*), instituindo-se instrumentos por meio dos quais os indivíduos pudessem identificar “o uso indevido de suas informações pessoais e propor a sua tutela”.<sup>101</sup>

Com o passar do tempo, o intenso emprego de técnicas e tecnologias computacionais de tratamentos de dados foi se tornando costume tanto por parte dos órgãos governamentais quanto por parte das entidades privadas, o que qualificou o fornecimento massivo de dados pessoais como uma condição *sine qua non* para o exercício de direitos pelo cidadão e para sua participação na vida social. Tal cenário fomentou, no início da década de 1980, o desenvolvimento de uma *terceira geração* de leis protetivas, a qual objetivou aperfeiçoar o quadro normativo de proteção dos dados pessoais e garantir a efetividade da “liberdade de

---

<sup>100</sup> *ibidem*, p. 40.

<sup>101</sup> *ibidem*, p. 41-42.

fornecer ou não os próprios dados pessoais”. Isso possibilitava o real respeito à autodeterminação informativa do cidadão.<sup>102</sup>

Todavia, a efetividade almejada pela terceira geração de leis apenas foi vivenciada por uma diminuta parcela dos cidadãos, uma vez que acionar os instrumentos para a defesa do direito à proteção dos dados e autodeterminação informativa era uma tarefa que demandava custos econômicos e pessoais – o que era oneroso demais para a maioria da população. Abriu-se espaço, pois, para a quarta geração de leis, que se dedicou ao desafio de “suprir as desvantagens do enfoque individual existente até então” e muitas são adotadas até hoje por diversos países. Destacam-se como características próprias dessa quarta geração: (i) o reconhecimento do desequilíbrio de forças entre os titulares dos dados pessoais e as instituições (públicas ou privadas) responsáveis pela coleta e processamento dos dados, com o consequente fortalecimento das prerrogativas dos cidadãos; (ii) a tutela diferenciada oferecida aos dados pessoais sensíveis; (iii) a instituição e o papel de destaque de autoridades independentes encarregadas de fazer valer a aplicação das leis que regulam o tratamento dos dados pessoais e o exercício efetivo da autodeterminação informativa.<sup>103</sup>

No que tange aos exemplos de diplomas legais integrantes dessa quarta geração, merece destaque o modelo adotado pela União Europeia por meio da Diretiva 95/46/CE (já revogada) e pelo seu substituto e atual norma regente dos aspectos gerais de proteção de dados nos países do bloco europeu: o *General Data Protection Regulation* (GDPR)<sup>104</sup>, o qual serviu de inspiração para a edição da Lei Geral de Proteção de Dados brasileira (LGPD). As semelhanças entre o GDPR e a LGPD serão brevemente tratadas no tópico 4.2 do presente trabalho.

Revela-se, ademais, indispensável uma abordagem, ainda que sucinta, do tema relativo aos princípios de proteção dos dados pessoais.

Stefano Rodotà assevera que seria possível extrair um “núcleo comum” a respeito da disciplina jurídica da proteção de dados tomando-se por base dois documentos marcantes: a Convenção do Conselho da Europa de 28 de janeiro de 1981 (também conhecida como

---

<sup>102</sup>*ibidem*.

<sup>103</sup>*ibidem*.

<sup>104</sup>*ibidem*, p. 42-43.

Convenção de Estrasburgo ou Convenção n. 108 do Conselho da Europa), para a proteção das pessoas em relação à coleta automática de dados de caráter pessoal, e a Recomendação da OCDE de 23 de setembro de 1980, na qual foram fixadas diretrizes relativas à proteção da vida privada e à circulação transnacional dos dados de caráter pessoal (*Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais*).<sup>105</sup>

De acordo com Rodotà os pontos em comum entre esses dois documentos de relevância internacional permitem a dedução dos seguintes princípios:

1. princípio da correção na coleta e no tratamento das informações;
2. princípio da exatidão dos dados coletados, acompanhado pela obrigação de sua atualização;
3. princípio da finalidade da coleta dos dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (princípio da pertinência); na relação entre a finalidade da coleta e a utilização dos dados (princípio da utilização não-abusiva); na eliminação, ou na transformação em dados anônimos das informações que não são mais necessárias (princípio do direito ao esquecimento);
4. princípio da publicidade dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
5. princípio do acesso individual, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
6. princípio da segurança física e lógica da coletânea dos dados.<sup>106</sup>

No magistério de Doneda, os aludidos princípios:

[...] formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados pessoais, formando o núcleo de questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais.<sup>107</sup>

A Lei Geral de Proteção de Dados brasileira – LGDP (Lei n.º 13.709/2018), nessa linha, traz em seu bojo uma série de princípios de proteção de dados a serem observados na atividade de tratamento de dados e que claramente guardam relação com os princípios supracitados.

Veja-se o que dispõe o seu artigo 6º:

<sup>105</sup> RODOTÀ, S., *op. cit.*, p. 59.

<sup>106</sup> *ibidem*.

<sup>107</sup> DONEDA, D. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.ª ed. Indaiatuba: Editora Foco, 2019, p. 40.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: 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;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Nesse sentido, nota-se que, pelo que dispõe a Lei Geral de Proteção de Dados, qualquer atividade de tratamento de dados que se enquadre nas hipóteses por ela previstas (o alcance da LGPD será explicitado mais à frente, no subcapítulo 3.2) deverá observar os princípios acima transcritos, sob pena de se considerar ilícito o tratamento que não observe os princípios de proteção de dados pessoais.

### 3.1.2 A proteção de dados pessoais no ordenamento jurídico brasileiro

Conforme já visto no subcapítulo 2.3 do presente trabalho, no Brasil, o direito à proteção de dados pessoais não encontra previsão direta na Constituição Federal. O que há é uma tutela jurídica reflexa, a qual se dá a partir da interpretação sistemática dos artigos 1º, inciso III; 3º, incisos I e IV; 5º, X, XII e LXXII, a seguir transcritos:

Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:

(...) III - a dignidade da pessoa humana;

<sup>1</sup> Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil:

I - construir uma sociedade livre, justa e solidária;

(...)

IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.

<sup>1</sup> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

(...)

X - **são invioláveis a intimidade, a vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

(...)

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; (Vide Lei nº 9.296, de 1996)

(...)

LXXII - conceder-se-á **habeas data**:

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; [grifo nosso]

Doneda destaca que, sob um ponto de vista mais amplo, no âmbito do seu artigo 5º, incisos IX, XIV, XXXIII, XXXIV<sup>108</sup> e do artigo 220<sup>109</sup>, “a Constituição Federal contempla o problema da informação inicialmente através das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, o direito à privacidade”.<sup>110</sup>

Conforme visto anteriormente, o direito à proteção de dados pessoais e à autodeterminação informativa podem ser concebidos como expressões ou ramificações do princípio da dignidade da pessoa humana (um dos fundamentos sob os quais se assenta a

<sup>108</sup>BRASIL, 1988: “Art. 5º [...]”

IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; [...]

XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional;

XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; [...]

XXXIV - são a todos assegurados, independentemente do pagamento de taxas:

a) o direito de petição aos Poderes Públicos em defesa de direitos ou contra ilegalidade ou abuso de poder;

b) a obtenção de certidões em repartições públicas, para defesa de direitos e esclarecimento de situações de interesse pessoal; [...]

<sup>109</sup>BRASIL, 1988: “Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

§ 1º Nenhuma lei conterà dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

§ 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.”

<sup>110</sup>DONEDA, D. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.ª ed. Indaiatuba: Editora Foco, 2019, p. 40.

República, vide art. 1º, III da CF), tendo em vista que os dados pessoais caracterizam-se como uma extensão da personalidade. Logo, qualquer violação ou tratamento indevido de dados relacionados a uma pessoa natural representa uma violação à própria dignidade humana e ao livre desenvolvimento da personalidade.

Qualquer pessoa natural ou entidade pública ou privada que realize operações de tratamento de dados pessoais não poderá fazer tais atividades com fins discriminatórios ou abusivos, sendo vedadas pelo ordenamento práticas que denotem ou incorporem “preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação” (art. 3º, IV da CF c/c art. 6º, IX da LGPD).

A inviolabilidade do direito à intimidade e à vida privada – tal como expresso pelo inciso X do art. 5º da Constituição – denotam o sentido clássico do direito à privacidade, que “consiste num direito a ser deixado em paz, ou seja, na proteção de uma esfera autônoma da vida privada, na qual o indivíduo pode desenvolver a sua individualidade [...] sem que ele seja compelido a determinados comportamentos socialmente esperados”.<sup>111</sup>

Assim, na linha do que já se expôs nos capítulos acima, verifica-se a identidade conceitual entre o direito à privacidade e o direito à proteção de dados pessoais. E a referida semelhança é ressaltada pela constatação de Canotilho e Vital, que subdividem

[...] o direito à reserva da intimidade da vida privada e familiar [...] em dois direitos menores: (a) o direito a impedir o acesso de estranhos a **informações sobre a vida privada e familiar de outrem**. Alguns outros direitos fundamentais funcionam como garantias deste: é o caso do direito à inviolabilidade do domicílio e da correspondência, **da proibição de tratamento informático de dados referentes à vida privada**. Instrumentos jurídicos privilegiados de garantia deste direito são igualmente o sigilo profissional e o dever de reserva das cartas confidenciais e demais papéis pessoais. [grifo nosso]<sup>112</sup>

Já o inciso XII do art. 5º da CF, ao dispor sobre a inviolabilidade do sigilo das comunicações em geral (inclusive da comunicação de dados), “abrange todas as espécies de comunicação pessoal, seja ela escrita ou oral, cobrindo tanto o conteúdo quanto o próprio

---

<sup>111</sup>SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D., *op. cit.*, p. 574.

<sup>112</sup>CANOTILHO, J. J. G. e VITAL, M. *apud* SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D., *op. cit.*, p. 574-575.

meio (instrumento) da comunicação, portanto, a espécie, a hora, a duração etc., mas também a identidade dos comunicantes”.<sup>113</sup>

Válido ressaltar, ademais, que o inciso LXXII do art. 5º da Carta da República introduz no ordenamento jurídico brasileiro o “remédio constitucional” do *Habeas Data* – posteriormente regulamentado pela Lei nº 9.507/1997, o qual, no parecer de Doneda, “visa a assegurar um direito presente em nosso ordenamento jurídico, ainda que não expresso literalmente”. Por meio dele, o cidadão pode acessar e retificar seus dados pessoais em bancos de dados “de entidades governamentais ou de caráter público”.<sup>114</sup> No que tange à sua efetividade, o autor em questão aponta que a referida ação:

[...] não é acompanhada [...] de instrumentos que possam torna-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais: além do seu perfil estar demasiadamente associado à proteção de liberdades negativas, [...] ela é, substancialmente, um instrumento que proporciona uma tutela pouco adequada à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação. [...]<sup>115</sup>

No que se refere ao quadro normativo infraconstitucional, merecem destaque algumas leis que tratam, ainda que indiretamente, de aspectos relacionados à proteção dos dados pessoais.

A primeira delas é a Lei nº 8.708/1990, mais conhecida como Código de Defesa do Consumidor – CDC. O código consumerista brasileiro traz em seu bojo disposições normativas em torno do direito de acesso às informações que digam respeito ao consumidor, com a indicação da respectiva fonte, além de dispor sobre requisitos para a criação e/ou manutenção de cadastros e bases de dados relativas aos consumidores, direito de retificação de dados cadastrais inexatos ou incorretos, dentre outras prescrições.

As disposições em questão estão inseridas na Seção VI (“Dos Bancos de Dados e Cadastros de Consumidores”) do Capítulo V (Das Práticas Comerciais) do CDC, a seguir transcrita:

---

<sup>113</sup>SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D., *op. cit.*, p. 596.

<sup>114</sup>DONEDA, D. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.<sup>a</sup> ed. Indaiatuba: Editora Foco, 2019, p. 49.

<sup>115</sup>*ibidem*.

Art. 43. **O consumidor [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.**

§ 1º Os **cadastros e dados de consumidores** devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

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

§ 3º **O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção**, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

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

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015)

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

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

§ 2º Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código. [...] [grifo nosso]<sup>116</sup>

Aproximadamente doze anos depois, surge o Código Civil atualmente em vigor (Lei n.º 10.406/2002). Diferentemente do Código de Civil de 1916 – que não trouxe qualquer previsão a respeito do direito à intimidade, à vida privada ou a qualquer direito da personalidade, dado o seu caráter eminentemente patrimonialista<sup>117</sup> –, o Código Civil de 2002 (CC/02) trouxe várias disposições a respeito dos direitos da personalidade – aí incluído o direito à privacidade.

Conforme exposto no subcapítulo 2.2 deste trabalho, o CC/02 não enuncia expressamente o direito à proteção de dados pessoais, e sim dedica um capítulo (Capítulo III – Dos Direitos da Personalidade, Título I – Das pessoas naturais, Livro I – Das Pessoas) para dispor, em rol não taxativo, sobre os direitos da personalidade (vide artigos 11 a 21). Há, portanto, apenas uma tutela reflexa dos dados pessoais a partir da interpretação do art. 12

<sup>116</sup>BRASIL. **Lei n. 8.078, de 11 de setembro de 1990 [Código de Defesa do Consumidor]**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/18078.htm](http://www.planalto.gov.br/ccivil_03/leis/18078.htm). Acesso em: 23 nov. 2019.

<sup>117</sup>BRASIL. **Lei n. 3.071, de 1º de janeiro de 1916 [Código Civil de 1916]**. Código Civil dos Estados Unidos do Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/13071.htm](http://www.planalto.gov.br/ccivil_03/leis/13071.htm). Acesso em: 23 nov. 2019.

combinado com o art. 21 do Código Civil, os quais garantem a proteção do direito à privacidade (na acepção de “vida privada”), *in verbis*:

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

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

Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.<sup>118</sup>

Nesse sentido, de acordo com as reflexões de Maria Celina Bodin de Moraes, “a ampliação dos direitos da personalidade, no nível do Civil de 2002, deve se atribuir ao art. 21, interpretando-se a ‘inviolabilidade da vida privada’ não como a tímida tutela do microcosmo da casa, mas como o espaço (inviolável) da liberdade de escolhas existenciais”.<sup>119</sup> E, pelo que se expôs até aqui, nota-se que o direito à proteção dos dados pessoais insere-se, de modo satisfatório, nesse escopo da “liberdade de escolhas existenciais”.

Prosseguindo-se com a breve investigação acerca dos diplomas normativos infraconstitucionais que abordam algum aspecto da proteção dos dados pessoais, vê-se que, em sentido parecido com as disposições do Código de Defesa do Consumidor, a Lei n.º 12.414/2011 – denominada Lei do Cadastro Positivo – dispõe sobre “a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito”.<sup>120</sup>

Trata-se da regulação, pelo ordenamento brasileiro, do chamado sistema de *Credit Scoring*, fruto da sociedade do consumo, na qual a procura do crédito atua como condição de possibilidade para que o indivíduo “consumidor” possa participar da engrenagem da circulação e aquisição de bens e serviços. Ele – o *Credit Scoring* – pode ser definido como:

<sup>118</sup>BRASIL. **Lei n. 10.406, de 10 de janeiro de 2002 [Código Civil de 2002]**. Institui o Código Civil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm). Acesso em: 23 nov. 2019.

<sup>119</sup>MORAES, M. C. B.. Ampliando os direitos da personalidade. **ResearchGate**, 2010, p. 5-6. Disponível em: [https://www.researchgate.net/publication/288490662\\_Ampliando\\_os\\_direitos\\_da\\_personalidade](https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade). Acesso em: 02 nov. 2019.

<sup>120</sup>BRASIL. **Lei n.º 12.414, de 9 de junho de 2011 [Lei do Cadastro Positivo]**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112414.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm). Acesso em: 23 nov. 2019.

[...] um mecanismo de *profiling* [definição de perfis com base na análise de dados pessoais] que enfoca especificamente a análise de crédito de pequenos valores. Criado com a finalidade de garantir maior segurança e agilidade às operações de crédito, o sistema opera atribuindo uma pontuação ao consumidor que pleiteia crédito, com base em técnicas estatísticas, mais especificamente por meio de um algoritmo. Tal pontuação, por sua vez, serve como um indicativo ao proponente do crédito acerca do risco (de inadimplimento) que a operação envolve.<sup>121</sup>

Assim, o art. 3º da Lei do Cadastro Positivo institui um permissivo legal para a criação de bancos de dados que armazenem informações creditícias da pessoa cadastrada, com o intuito de se constituir um “histórico de crédito”. Eis o seu teor:

Art. 3º Os bancos de dados poderão conter informações de adimplimento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.

§ 1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado. [...]

Ainda sobre a Lei do Cadastro Positivo, Fernando Machado afirma que o diploma legal em questão “está em harmonia com um direito à proteção dos dados pessoais, não só em termos de Brasil, mas de União Europeia”, na medida em que, em sua análise, pela leitura dessa lei seria possível identificar diversos princípios da proteção de dados pessoais<sup>122</sup>, dentre eles:

[...] o **dever de objetividade e clareza das informações armazenadas** (art. 3º, §1º); a vedação de anotações de informações excessivas, consubstanciada no **princípio da adequação** (art. 3º, §3º, inciso I)<sup>123</sup>; a **vedação de anotações sensíveis** (art. 3º, §3º, inciso II); o **princípio do consentimento informado** (arts. 4º<sup>124</sup>, 9º<sup>125</sup> e

<sup>121</sup> MACHADO, F. I. S. **Privacidade e proteção de dados pessoais na sociedade da informação: profiling e risco de discriminação**. 2018. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018, p. 146.

<sup>122</sup> MACHADO, F. I. S., *op. cit.*, p. 145-146.

<sup>123</sup>“Art. 3º [...] § 3º Ficam proibidas as anotações de:

I - informações excessivas, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e  
II - informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.”.

<sup>124</sup> “Art. 4º O gestor está autorizado, nas condições estabelecidas nesta Lei, a:

I - abrir cadastro em banco de dados com informações de adimplimento de pessoas naturais e jurídicas;  
II - fazer anotações no cadastro de que trata o inciso I do caput deste artigo;  
III - compartilhar as informações cadastrais e de adimplimento armazenadas com outros bancos de dados; e  
IV - disponibilizar a consulentes:  
a) a nota ou pontuação de crédito elaborada com base nas informações de adimplimento armazenadas; e

11<sup>126</sup>); os **direitos de acesso às informações e de retificação das mesmas** (art. 5<sup>o127</sup>, incisos II e III); o **princípio da finalidade** (art. 5<sup>o</sup>, inciso VII, e art. 7<sup>o128</sup>), e o **dever de apagamento dos dados** (art. 14)<sup>129</sup>. [...] [grifo nosso]  
130

Pouco tempo depois de a Lei do Cadastro Positivo ter sido sancionada, no mesmo ano de 2011 entrou em vigor a Lei de Acesso à Informação (LAI) – Lei nº 12.527/2011<sup>131</sup>. Esta lei, como o nome sugere, tem o propósito de regular e garantir o “direito fundamental de acesso à informação” (art. 3<sup>o</sup>, *caput*), especificamente no que diz respeito aos “procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5<sup>o</sup>, no inciso II do § 3<sup>o</sup> do art. 37 e no § 2<sup>o</sup> do art. 216 da Constituição Federal”, conforme estipulado em seu art. 1<sup>o</sup>, *caput*. O referido dispositivo também prevê, em seu parágrafo único, o âmbito de incidência da Lei de Acesso à Informação, isto é, aponta os sujeitos que a ela estão subordinados, como se vê abaixo:

Art. 1<sup>o</sup>[...] Parágrafo único. Subordinam-se ao regime desta Lei:

---

b) o histórico de crédito, mediante prévia autorização específica do cadastrado. [Redação dada pela L.C. nº 166/2019]”.

<sup>125cc</sup> Art. 9<sup>o</sup> O compartilhamento de informações de adimplemento entre gestores é permitido na forma do inciso III do caput do art. 4<sup>o</sup> desta Lei. [...] [Redação dada pela L.C. nº 166/2019]”.

<sup>126</sup>Revogado pela Lei Complementar nº 166, de 2019.

<sup>127cc</sup> Art. 5<sup>o</sup> São direitos do cadastrado: [...]

II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;

III - solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação; [...] [Redação dada pela L.C. nº 166/2019]

VI - solicitar ao consultante a revisão de decisão realizada exclusivamente por meios automatizados; ”.

<sup>128</sup> Art. 7<sup>o</sup> As informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para:

I - realização de análise de risco de crédito do cadastrado; ou

II - subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consultante.

Parágrafo único. Cabe ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta para informar aos consultantes as informações de adimplemento do cadastrado.”.

<sup>129cc</sup> Art. 14. As informações de adimplemento não poderão constar de bancos de dados por período superior a 15 (quinze) anos.”.

<sup>130</sup>MACHADO, F. I. S., *op. cit.*, p. 145.

<sup>131</sup>BRASIL. **Lei n. 12.527, de 18 de novembro de 2011 [Lei de Acesso à Informação]**. Regula o acesso a informações previsto no inciso XXXIII do art. 5<sup>o</sup>, no inciso II do § 3<sup>o</sup> do art. 37 e no § 2<sup>o</sup> do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm). Acesso em: 23 nov. 2019.

- I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
- II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Tais sujeitos, conforme se depreende da leitura do dispositivo acima transcrito, são, geralmente, pessoas jurídicas de direito público ou pessoas jurídicas de direito privado que tenham algum tipo de vínculo com a administração direta dos poderes constituídos do Estado (v.g., sociedades de economia mista e empresas públicas).

Ademais, as disposições da aludida lei aplicam-se, no que couber, “às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres”, na linha do que reza o seu art. 2º, *caput*.

O art. 4º, por seu turno, preocupa-se em definir alguns termos referenciados na própria LAI, merecendo destaque as definições de informação, informação pessoal e tratamento da informação, a seguir e respectivamente transcritos:

Art. 4º Para os efeitos desta Lei, considera-se:

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; [...]

IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; [...]

Outro dispositivo normativo relevante é aquele que estabelece os parâmetros a serem observados quando do tratamento das informações pessoais, demandando respeito ao direito à privacidade e às liberdades e garantias individuais, conforme prescreve o art. 31 da Lei de Acesso à Informação:

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

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

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

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

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

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

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

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

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

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

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal. [grifo nosso]

Por fim, encerrando este breve panorama sobre os marcos normativos do direito à privacidade e à proteção de dados pessoais no ordenamento jurídico brasileiro, há que se fazer menção à Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet (MCI)<sup>132</sup>, que se propõe a estabelecer “princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria” (art. 1º).

O Marco Civil da Internet está fundamentado principalmente no respeito à liberdade de expressão, como ressalta o seu art. 2º, o qual, em seus incisos, indica outras bases sobre as quais se estruturam o seu escopo normativo, quais sejam:

[...] I - o reconhecimento da escala mundial da rede;

II - os **direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;**

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede. [grifo nosso]

<sup>132</sup>BRASIL. **Lei nº 12.965, de 23 de abril de 2014 [Marco Civil da Internet]**. 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: 23 nov. 2019.

O referido diploma legal serviu para preencher uma lacuna existente na legislação brasileira, definindo os direitos e deveres relativos à regulação e ao uso da rede mundial de computadores – *Internet* – no Brasil.

Sublinhe-se que é possível identificar na lei em tela pontos de contato com o direito à proteção de dados pessoais e à autodeterminação informativa, uma vez que o Marco Civil elegeu a proteção da privacidade e a proteção dos dados pessoais dentre os princípios acerca da disciplina do uso da internet no Brasil (art. 3º, caput, incisos II e III).

Além disso, assegurou, dentre outros, os seguintes direitos dos usuários de internet (art. 7º):

[...] I - **inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;**

II - **inviolabilidade e sigilo do fluxo de suas comunicações pela internet**, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]

VII - **não fornecimento a terceiros de seus dados pessoais**, inclusive registros de conexão, e de acesso a aplicações de internet, **salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;**

VIII - **informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para **finalidades** que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - **consentimento expresso** sobre **coleta, uso, armazenamento e tratamento de dados pessoais**, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - **exclusão** definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; [...] [grifo nosso]<sup>133</sup>

Nesse sentido, Teffé destaca que, para além da liberdade de expressão, a privacidade e a neutralidade da rede também figuram como fundamentos do Marco Civil da Internet. Com isso:

[...] pode-se afirmar que os pilares da Lei estão pautados pelo direito de externar ideias, juízos de valor e as mais variadas manifestações do pensamento, **na possibilidade de a pessoa natural controlar a circulação de suas informações e dados pessoais [Rodotà], bem como impedir a intromissão de terceiros ou do**

<sup>133</sup> *ibidem*.

**Estado em sua vida íntima;** e em “princípio de arquitetura de rede que endereça aos provedores de acesso o dever de tratar os pacotes de dados que trafegam em suas redes de forma isonômica, não os discriminando em razão de seu conteúdo, origem, destino ou tipo de aplicação”. [grifo nosso] <sup>134</sup>

Verifica-se, no entanto, que Marco Civil da Internet não se concebe como uma norma geral sobre proteção de dados pessoais, trazendo apenas algumas disposições sobre proteção de dados, muitas delas de natureza apenas enunciativa, sem a efetiva previsão de um escopo protetivo ao tratamento de dados relacionados aos indivíduos.

Isso fica claro ao se realizar a leitura do art. 3º, inciso III, o qual preconiza que a “disciplina do uso da internet no Brasil” tem entre seus princípios a “proteção dos dados pessoais, **na forma da lei**” [grifo nosso].

Esta lei veio a ser sancionada aproximadamente quatro anos após a edição do MCI, e é exatamente sobre ela, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), que versará o próximo subcapítulo do presente trabalho.

### 3.2 Fundamentos, objetivos, alcance, principais conceitos e direitos enunciados pela Lei Geral de Proteção de Dados

Segundo consta no Considerando de nº (6) e (7) do Regulamento Geral de Proteção de Dados da União Europeia (mais conhecido como GDPR, i.e., *General Data Protection Regulation*):

(6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

(7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a

---

<sup>134</sup>TEFFÉ, C. S. Marco Civil da Internet: considerações sobre a proteção da liberdade de expressão, neutralidade da rede e privacidade. *In*: BECKER, D.; FERRARI, I.; (Coord.). **Regulação 4.0**: Novas tecnologias sob a perspectiva regulatória. São Paulo: RT, 2019, p. 137.

segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.<sup>135</sup>

Tal cenário ilustra satisfatoriamente alguns dos efeitos dos novos arranjos sociais, económicos e políticos decorrentes da sociedade informacional que vêm se consolidando nas últimas décadas. De fato, o fornecimento dos dados pessoais tem se tornado comum no ambiente virtual, fazendo com que o indivíduo perca o controle sobre suas próprias informações, as quais frequentemente são repassadas a terceiros por questões comerciais, além de receberem os mais diversos tipos de tratamento de dados sem que os usuários estejam cientes disso.

Nesse contexto, verifica-se uma espécie de banalização ou descuido no fornecimento de dados pessoais por parte dos usuários no ambiente virtual, bem como o uso indiscriminado de tais dados pelas empresas e pelos próprios governos.

Dessa forma, abre-se espaço para que entidades privadas e públicas tornem-se capazes de estabelecer rótulos e de traçar padrões hábitos e de comportamentos dos indivíduos, o que dá ensejo a situações de violação aos direitos fundamentais dos cidadãos, especialmente em se tratando da análise dos dados sensíveis.

Um caso emblemático foi o vazamento de dados envolvendo o *Facebook*, que afetou cerca de 87 milhões de usuários dessa rede social e, dentre eles, foram afetados mais de 443 mil brasileiros. Os dados pessoais dessa parcela de usuários teriam sido repassados para a *Cambridge Analytica*, empresa que se dedicava à criação de campanhas políticas utilizando técnicas sofisticadas de análise de dados e de anúncios direcionados com o objetivo de influenciar o resultado do processo eleitoral nos países, favorecendo o candidato que contratasse seus serviços. Nesse caso específico, ocorrido em 2016, a *Cambridge Analytica* foi contratada pela assessoria do então candidato à presidência dos Estados Unidos da

---

<sup>135</sup> PARLAMENTO EUROPEU E DO CONSELHO. **Regulamento 2016/679**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e6949-1-1>. Acesso em: 23 nov. 2019.

América, Donald Trump, com o objetivo de influenciar o voto de potenciais eleitores, promovendo uma espécie de “guerra cultural”.<sup>136 137 138</sup>

No mesmo ano de 2016, no mês de abril, foi publicado o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), o qual, pelo disposto em seu art. 3º, é aplicável não apenas no âmbito dos Estados-membros da União Europeia, mas também a países estrangeiros que de algum modo realizem tratamento de dados de cidadãos europeus<sup>139</sup>.

No caso de empresas situadas no (ou vinculadas ao) Brasil, por exemplo, estas estariam obrigadas a seguir o GDPR em hipóteses envolvendo:

[...] subsidiárias de empresas europeias no Brasil que tratem dados de cidadãos europeus e pessoas que residam na Europa;  
empresas brasileiras que fizerem ou tiverem alguma transação que envolva dados pessoais com a Europa;  
empresas brasileiras que não fizeram transação alguma com a Europa, mas, em algum momento, tratarem dados de europeus, ainda que em solo brasileiro;  
[...] subsidiárias no Brasil de empresas não-europeias mas com presença na Europa [...]<sup>140</sup>

<sup>136</sup>CANO, R. J. Mais de 400 mil brasileiros foram afetados pelo vazamento de dados do Facebook. **El País**, Guadalajara, 05 abr. 2018. Tecnologia. Disponível em: [https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235\\_618558.html](https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235_618558.html). Acesso em: 23 nov. 2019.

<sup>137</sup>CAMBRIDGE Analytica se declara culpada em caso de uso de dados no Facebook. **G1**, 09 jan. 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml>. Acesso em: 23 nov. 2019. Economia, Tecnologia.

<sup>138</sup>ROSENBERG, M; CONFESSORE, N.; CADWALLADR, C. How Trump Consultants Exploited the Facebook Data of Millions. **The New York Times**, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 23 nov. 2019. Politics.

<sup>139</sup>PARLAMENTO EUROPEU E DO CONSELHO, 2016: “Art. 3º [...] 1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.”

<sup>140</sup>GOMES, H. S. Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda. **G1**, 25 maio 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>. Acesso em: 23 nov. 2019. Economia, Tecnologia.

Todos esses fatores influenciaram na celeridade dos trâmites legislativos para a edição de uma lei brasileira destinada apenas a regular os aspectos gerais da proteção de dados pessoais tomando como fonte inspiradora o GDPR<sup>141</sup>.

Dessa maneira, no dia 14 de agosto de 2018, foi sancionada a Lei nº 13.709/2018, que ficou conhecida como a Lei Geral de Proteção de Dados ou simplesmente LGPD (posteriormente alterada pela Lei nº 13.853/2019 e por outros instrumentos normativos), para dispor sobre “o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado” (art. 1º, *caput*), trazendo em seu bojo normas gerais de interesse nacional (art. 1º, parágrafo único).

Seu objetivo, expressamente declarado (art. 1º, *caput, in fine*), é o de “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da **pessoa natural**” [grifo nosso].

Assim, busca-se “conferir uma ampla proteção ao cidadão e às situações existenciais mais importantes que são afetadas pelo tratamento de dados”,<sup>142</sup> tendo em vista que “o eixo valorativo da LGPD é a proteção da pessoa humana e de suas situações existenciais, o que deve ser levado em consideração para a interpretação de todas as suas demais disposições”.<sup>143</sup>

Acerca do quadro normativo brasileiro de proteção de dados pessoais, afigura-se pertinente explicitar a análise de Bruno Bioni, o qual assevera que:

[...] Até a aprovação da LGPD, o Brasil contava somente com leis setoriais de proteção de dados. Era uma verdadeira “colcha de retalhos” que não cobria setores importantes da economia e, dentre aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para: a) que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios; b) a formulação de políticas públicas e parcerias público-privadas igualmente dependentes desse intercâmbio de dados; e c) o cidadão que não detinha uma proteção integral e universal com relação a todas as atividades do cotidiano em que fornece seus dados, seja para o setor privado ou público.<sup>144</sup>

<sup>141</sup> Nesse sentido: SOUZA, L. R. M. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro n. 5.276/2016. **Caderno Virtual, IDP, Brasília** – DF, v.1, n. 41, 2018. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153/1484>. Acesso em: 23 nov. 2019.

<sup>142</sup> FRAZÃO, A. Objetivos e alcance da Lei geral de Proteção de Dados. In: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 102.

<sup>143</sup> *ibidem*, p. 104.

<sup>144</sup> BIONI, B., *op. cit.*, p.133.

Seus fundamentos estão expressos no art. 2º, como se verifica abaixo:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:  
I - o respeito à privacidade;  
II - a autodeterminação informativa;  
III - a liberdade de expressão, de informação, de comunicação e de opinião;  
IV - a inviolabilidade da intimidade, da honra e da imagem;  
V - o desenvolvimento econômico e tecnológico e a inovação;  
VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e  
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Vê-se, pois, que o propósito da LGPD é, a um só tempo, proteger direitos e garantias fundamentais como o respeito à privacidade, à autodeterminação informativa, ao regime de liberdades individuais e à defesa do consumidor, bem como promover o desenvolvimento econômico e tecnológico, a livre iniciativa e a inovação, pavimentando um terreno em que possam coexistir interesses que muitas vezes aparentam ser antagônicos.

Nesse contexto, é oportuno mencionar o que Bioni denomina de a “dupla função” das normas de proteção de dados pessoais: (i) garantia da privacidade e de outros direitos fundamentais e (ii) fomento do desenvolvimento econômico. Dessa forma, as referidas normas protetivas, de uma maneira geral, “procuravam conferir segurança jurídica tanto ao cidadão, como, também, ao setor estatal e privado sobre como deve se dar o fluxo desses dados. E, em última análise, assegurar confiança entre todos os atores desse ecossistema [...]”.<sup>145</sup>

O que se percebe, numa leitura constitucional, é que a LGPD, no que diz respeito aos seus objetivos, reforça os objetivos fundamentais da própria República (art. 3º da Constituição Federal), viabilizando-se o projeto de construção de uma sociedade livre, justa e solidária, de promoção do bem de todos sem quaisquer formas de discriminação e de garantia do desenvolvimento nacional.

Para o satisfatório alcance de tais objetivos, o “principal vetor [...] é franquear ao cidadão controle sobre seus dados pessoais”, assegurando-se “**que o fluxo informacional**

---

<sup>145</sup>BIONI, B., *op. cit.*, p.132-133.

atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade” [grifo nosso].<sup>146</sup>

No que se refere ao seu âmbito de aplicação, a Lei Geral de Proteção de Dados, na linha do que estipula o seu art. 3º, *caput*, alcança:

[...] **qualquer operação de tratamento** realizada por pessoa **natural** ou por pessoa **jurídica** de direito público ou privado, **independentemente do meio**, do país de sua sede ou do país onde estejam localizados os dados, **desde que**:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do *caput* do art. 4º desta Lei. [grifo nosso]

Logo, estão sujeitos às disposições da LGPD toda e qualquer pessoa natural ou jurídica (sob qualquer regime) que realizem alguma operação de tratamento de dados pessoais, em meio digital ou físico, que se enquadrem nas condições estipuladas pelos incisos I a III do supracitado art. 3º.

Além disso, para prevenir qualquer tipo de controvérsia, o art. 1º, parágrafo único, deixa claro que os entes públicos não escapam de seu âmbito normativo, ao dispor que as “normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios”.

Ressalta-se, ademais, que a lei em questão aponta em quais hipóteses ela não será aplicável. Desse modo, para escapar dos “tentáculos” da LGPD, o tratamento de dados a ser realizado precisa estar adstrito a certas finalidades constantes dos incisos do art. 4º, *in verbis*:

Art. 4º Esta Lei **não se aplica** ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

<sup>146</sup>*ibidem*, p. 134.

- b) defesa nacional;  
 c) segurança do Estado; ou  
 d) atividades de investigação e repressão de infrações penais; ou  
 IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. [...] [grifo nosso]

É importante fazer menção, também, aos conceitos constantes da Lei Geral de Proteção de Dados, os quais estão contidos no art. 5º. Eis algumas definições importantes constantes da tabela elaborada a seguir:

**Tabela 1 – Principais conceitos constantes da Lei Geral de Proteção de Dados (LGPD).**

<b>Expressão</b>	<b>Conceito</b>	<b>Base legal</b>
<b>Dado pessoal</b>	Informação relacionada a pessoa natural identificada ou identificável.	Art. 5º, inciso I
<b>Dado pessoal sensível</b>	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.	Art. 5º, inciso II
<b>Dado anonimizado</b>	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.	Art. 5º, inciso III
<b>Banco de dados</b>	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.	Art. 5º, inciso IV
<b>Titular</b>	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.	Art. 5º, inciso V
<b>Controlador</b>	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.	Art. 5º, inciso VI

<b>Operador</b>	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.	Art. 5º, inciso VII
<b>Encarregado</b>	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).	Art. 5º, inciso VIII
<b>Agentes de tratamento</b>	O controlador e o operador.	Art. 5º, inciso IX
<b>Tratamento</b>	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.	Art. 5º, inciso X
<b>Anonimização</b>	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.	Art. 5º, inciso XI
<b>Consentimento</b>	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.	Art. 5º, inciso XII
<b>Bloqueio</b>	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.	Art. 5º, inciso XIII
<b>Eliminação</b>	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.	Art. 5º, inciso XIV

Fonte: Própria (2020).

Como bem observa Ana Frazão, a presente lei tem o intuito de “regular todas as formas de tratamento de dados pessoais, [...] incluindo até mesmo aqueles considerados públicos ou tornados públicos pelos titulares”.<sup>147 148</sup>

Pela leitura das definições anteriormente transcritas, nota-se que a LGPD adota a nomenclatura “titular” dos dados para fazer referência, em seus próprios termos, à “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (art. 5º, V).

Rodotà, por exemplo, critica a transposição de uma lógica patrimonial a questões eminentemente existenciais. Isso porque, para ele, haveria, contemporaneamente, uma “tendência de inserir o direito à privacidade entre os instrumentos de tutela da personalidade, desprendendo-o de uma orientação que o vincule ao direito de propriedade”.<sup>149</sup> Prossegue afirmando, ainda, que a “possibilidade de manter um controle integral sobre as próprias informações, de fato, contribui de modo determinante para definir a posição do indivíduo na sociedade”.

Poder-se-ia inferir, a partir disso, que o emprego do termo “titular dos dados” soaria inadequado. No entanto, conforme ressaltam Souza e Silva, o emprego do termo “titular” não é de todo inoportuno:

[...] tendo em vista a necessidade de identificar com clareza os sujeitos a que se refere a lei. A rigor, considerando que a titularidade consiste no vínculo que une o indivíduo a toda situação jurídica, de qualquer natureza (patrimonial ou existencial), o uso do termo em matéria extrapatrimonial mostra-se tão adequado quanto à referência a situações jurídicas nesse setor (e a lei, neste particular, remete claramente à estipulação de direitos).<sup>150</sup>

<sup>147</sup>FRAZÃO, A. Objetivos e alcance da Lei geral de Proteção de Dados. In: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 102.

<sup>148</sup>Essa constatação a respeito da incidência da LGPD sobre o tratamento dos dados pessoais tornados públicos advém da leitura dos §§3º e 4º do art. 7º:

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

§ 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

§ 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.[...]”.

<sup>149</sup>RODOTÀ, S. **A vida na sociedade da vigilância**: A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 98

<sup>150</sup>SOUZA, E. N.; SILVA, R. G. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direito e a enunciação de remédios. **Pensar**, Fortaleza, v. 24, n. 3, p.1-22, jul./set. 2019, p. 8. Disponível em: <https://periodicos.unifor.br/rpen/article/view/9407>. Acesso em: 02 nov. 2019.

Uma parte de indubitável importância na topografia da Lei Geral de Proteção de Dados é aquela destinada à previsão dos direitos do titular dos dados (Capítulo III – Dos Direitos do Titular), estendendo-se dos artigos 17 a 22.

Nesse ponto, afigura-se pertinente trazer à tona as reflexões de Souza e Silva no sentido de que a leitura de tais disposições permitiria concluir que a LGPD, muito mais do que atribuir direitos, dedica-se a, na verdade, enunciar remédios atrelados à tutela de direitos que já haviam sido incorporados pelo ordenamento jurídico brasileiro, com destaque para o direito à privacidade e suas múltiplas facetas.<sup>151</sup>

Segundo tais autores, o exame de um caso concreto pressupõe a elaboração de dois questionamentos: (i) “[o] exercício da situação jurídica ora reconhecida é **merecedor de tutela?**” [grifo nosso]; e (ii) “[q]ual é a **exata medida da tutela** conferida ao exercício da situação jurídica em exame?”[grifo nosso]. Tais questionamentos são necessários tendo em vista que “a decisão sobre o merecimento de tutela não se completa de sentido sem a delimitação da medida da tutela a que se faz jus no caso concreto [...], e a disciplina prevista pela LGPD apenas destaca essa constatação”.<sup>152</sup>

De todo modo, impende assinalar que a análise mais detalhada acerca dos mecanismos de tutela dos direitos do titular dos dados será realizada no próximo capítulo do presente trabalho, oportunidade em que se explicitará a questão do “prisma remedial” adotado pela Lei Geral de Proteção de Dados.

Neste momento, cabe apenas abordar alguns dispositivos interessantes inseridos no capítulo que, na concepção do legislador, buscou atribuir “direitos” ao titular dos dados pessoais.

O art. 17 encarrega-se de enunciar que “[t]oda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da Lei”. Aqui, nota-se a LGPD tem como razão de

---

<sup>151</sup>*ibidem, passim.*

<sup>152</sup>*ibidem*, p. 2-3.

ser a “tutela de uma particular vulnerabilidade do mundo contemporâneo [...] ao atribuir expressamente certos direitos ao grupo vulnerável – os titulares de dados pessoais”.<sup>153</sup>

Em seguida, o art. 18 dedica-se a estipular os direitos do titular dos dados perante a figura do controlador<sup>154</sup>. Os direitos em questão vinculam-se aos dados do titular tratados pelo controlador e o seu exercício será feito “mediante requisição”. Ei-los:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador;

V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei nº 13.853, de 2019)

VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;

IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. [...]

Por sua vez, o art. 19 prevê que, também mediante simples requisição, o titular dos dados terá direito à confirmação de existência de seus dados pessoais e/ou direito ao acesso dos mesmos, com nível de detalhamento que varia de acordo com o tempo de resposta do controlador: se for imediata, o formato da resposta será simplificado; noutro giro, se a resposta for rica em detalhes (“declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento”), concede-se ao controlador o prazo de até 15 (quinze) dias úteis, a partir da data do requerimento (art. 19, II, da LGPD).

O art. 20 atribui ao titular dos dados um direito dotado de grande relevância ao presente trabalho (e que será devidamente analisado mais à frente). Cuida-se do direito a solicitar a “revisão de decisões tomadas unicamente com base em tratamento automatizado de dados

---

<sup>153</sup> *ibidem*.

<sup>154</sup> Conforme visto anteriormente, trata-se da “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI, da LGPD).

personais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos da sua personalidade” (art. 20, *caput*, da LGPD).

Por seu turno, os artigos 21 e 22 tratam de assegurar, respectivamente, que os “dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo”, bem como que a “defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva”.

### 3.3 Vigência dos dispositivos da LGPD

No que diz respeito à vigência da Lei Geral de Proteção de Dados, é importante ressaltar a publicação de instrumentos normativos (leis e Medidas Provisórias) que modificaram sucessivamente a *vacatio legis* dos dispositivos da LGPD.

Nesse ponto, verifica-se que a redação original da LGPD (Lei n. 13.709/2018) estabelecia, em seu art. 65, que tal lei entraria “em vigor após decorridos 18 (dezoito) meses de sua publicação oficial”. Assim, considerando que sua publicação ocorreu no dia **14.08.2018**, depreende-se que sua vigência *teria início* no dia **15.02.2020**.

Todavia, desde sua publicação até momento da conclusão do presente trabalho, o período de *vacatio legis* da LGPD sofreu três alterações.

Num primeiro momento, a Lei n. 13.853/2019 (resultante da conversão da Medida Provisória 869/2018) instituiu dois momentos distintos de vacância da lei: (i) **antecipou** a vigência dos artigos que tratam da criação, organização, funcionamento e atribuição de competências da Autoridade Nacional de Proteção de Dados – ANDP (artigos 55-A a 55-L) e do Conselho Nacional de Proteção de Dados – CNPD (artigos 58-A e 58-B) para o dia

**28.12.2018**; e (ii) **prorrogou** o período de vacância dos demais artigos da LGPD para 24 (vinte e quatro) meses após a sua publicação, isto é, para o dia **14.08.2020**.<sup>155</sup>

Num segundo momento, a Medida Provisória 959/2020 promoveu nova alteração na LGPD, **prorrogando** para o dia **03.05.2021** a vigência dos demais artigos da LGPD (salvo aqueles artigos que tratam de questões institucionais da ANPD e do CNPD, vigentes desde 28.12.2018).<sup>156</sup>

Já num terceiro momento, a Lei n. 14.010/2020 (que cuida do Regime Jurídico Emergencial e Transitório das relações de Direito Privado no período da pandemia de Covid-19) **prorrogou** para o dia **01.08.2021** a vigência dos dispositivos da LGPD que tratam das sanções administrativas a cargo da ANPD (artigos 52, 53 e 54).<sup>157</sup>

Desse modo, a redação atual do artigo 65 da LGPD, após as sucessivas alterações acima mencionadas, é retratada abaixo:

Art. 65. Esta Lei entra em vigor: (*Redação dada pela Lei nº 13.853, de 2019*)  
 I - **dia 28 de dezembro de 2018**, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (*Incluído pela Lei nº 13.853, de 2019*)  
 I-A – **dia 1º de agosto de 2021**, quanto aos arts. 52, 53 e 54; (*Incluído pela Lei nº 14.010, de 2020*)  
 II - **em 3 de maio de 2021**, quanto aos demais artigos. (*Redação dada pela Medida Provisória nº 959, de 2020*) [grifo nosso]

Ademais, a tabela a seguir busca ilustrar de modo mais claro a correlação dos assuntos tratados pela LGPD e seus respectivos prazos de vigência:

<sup>155</sup> BRASIL. **Lei 13.853 de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2019/Lei/L13853.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm). Acesso em: 21 jul. 2020.

<sup>156</sup> BRASIL. **Medida Provisória n. 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília, DF: Presidência da República, 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/mpv/mpv959.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm). Acesso em 21 jul. 2020.

<sup>157</sup> BRASIL. **Lei n. 14.010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidência da República, 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/lei/L14010.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm). Acesso em 21 jul. 2020.

**Tabela 2 – Quadro esquemático do período de *vacatio legis* dos dispositivos da Lei Geral de Proteção de Dados (LGPD).**

<b>Assunto</b>	<b>Artigos da LGPD</b>	<b>Data de vigência</b>
Criação, organização, funcionamento e competências da ANPD e do CNPD.	55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B.	<b>28.12.2018 (em vigor)</b>
Sanções administrativas aplicadas pela ANPD em caso de violação às normas da LGPD por parte dos agentes de tratamento de dados.	52, 53 e 54.	<b>01.08.2021</b>
Demais artigos da LGPD.	Todos, salvo os acima explicitados.	<b>03.05.2021</b>

Fonte: Própria (2020).

Vê-se, portanto, que a possibilidade de aplicação de multa, vista como uma das principais preocupações do setor privado, só se dará a partir do dia 01.08.2021, oferecendo um prazo adicional para que as empresas de um modo geral promovam adequações para atendimento integral dos mandamentos da Lei Geral de Proteção de Dados.

Da mesma forma, suspende-se, a princípio, a possibilidade de aplicação de sanções administrativas diversas de multa e das sanções previstas na Lei n. 8.112/1990, na Lei de Improbidade Administrativa (Lei n. 8.429/1992) e na Lei de Acesso à informação (Lei n. 12.527/2011), desde que tenham fundamento em infrações previstas pela LGPD (vide seu art. 52, §3º).

Isso representa uma chance adicional para que a máquina estatal realize a capacitação e qualificação de seus agentes, além de adequar seus procedimentos técnicos e administrativos na linha do que preconiza a LGPD.

Frise-se, no entanto, que a responsabilização de agentes das esferas públicas e privadas por tratamento indevido de dados ainda subsiste, mesmo com as prorrogações mencionadas anteriormente, haja vista que o Supremo Tribunal Federal já se manifestou favoravelmente ao reconhecimento da autonomia do direito à proteção de dados pessoais, cujo fundamento

normativo decorre diretamente da Constituição Federal, conforme será exposto no subcapítulo a seguir.

### 3.4 A manifestação do Plenário do Supremo Tribunal Federal acerca da temática da proteção dos dados pessoais: o caso da MP n. 954/2020

No dia 17.04.2020, foi publicada a Medida Provisória n. 954/2020<sup>158</sup>, a qual, segundo a sua ementa:

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.

Tal instrumento normativo determina às empresas de telefonia o dever de disponibilizar ao “IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas” (art. 2º, *caput*) para servirem ao seguinte propósito: “produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares” (art.2º, §1º).

Esses dados pessoais, de acordo com a própria Medida Provisória, deverão ter “caráter sigiloso” e “serão usados exclusivamente para a finalidade prevista no §1º do art. 2º”, ou seja, para atender ao escopo de “produção estatística oficial” (art. 3º, *caput* e incisos I e II).

Ocorre que, no dia 07.05.2020, o Plenário do Supremo Tribunal Federal (STF) referendou, por ampla maioria (10 votos a 1), a medida cautelar deferida nos autos das Ações Diretas de Inconstitucionalidade (ADIs) n. 6387, n. 6388, n. 6389, n. 6390 e n. 6393, todas com o objetivo de impugnar a validade dos dispositivos da MP n. 954/2020, objetivando a

---

<sup>158</sup>BRASIL. **Medida Provisória n. 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 21 jul. 2020.

declaração de inconstitucionalidade da determinação de compartilhamento de dados pessoais de milhões de brasileiros a serem tratados pelo IBGE.<sup>159</sup>

A ministra Rosa Weber, relatora da ADI n. 6387 (e das outras ações correlatas, com tramitação conjunta à ADI distribuída primeiramente), deferiu a medida cautelar requerida pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), determinando: (i) a suspensão da eficácia da Medida Provisória n. 954/2020; e (ii) a obrigação de o IBGE se abster “de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia”.<sup>160</sup>

Em sua decisão monocrática no bojo da ADI 6387 MC/DF, a Min. Rosa Weber reconheceu que os dados a serem repassados ao IBGE são classificados como dados pessoais, integrando “o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)”. Dessa maneira, quaisquer tipos de “manipulação e tratamento [...] hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional”.<sup>161</sup>

A ministra, inclusive, chega a fazer expressa menção a dispositivos da LGPD nos fundamentos de sua decisão, vide excerto abaixo transcrito:

Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, **no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)**, como fundamentos específicos da disciplina da proteção de dados pessoais . [grifo nosso]<sup>162</sup>

Em outro trecho, a julgadora, ao tecer considerações sobre as falhas da Medida Provisória impugnada, novamente faz referência à Lei Geral de Proteção de Dados, ressaltando, desta vez, que:

---

<sup>159</sup>BRASIL. Supremo Tribunal Federal. AÇÃO DIRETA DE INCONSTITUCIONALIDADE: ADI n. 6387/DF – Distrito Federal. Ministra Relatora: Rosa Weber. Brasília, DF: **Portal STF**, Processos, Andamentos, 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 23 jul. 2020.

<sup>160</sup>BRASIL. Supremo Tribunal Federal. AÇÃO DIRETA DE INCONSTITUCIONALIDADE: ADI n. 6387/DF – Distrito Federal. Ministra Relatora: Rosa Weber. Brasília, DF: **Portal STF**, Processos, Decisões, 2020, p.12. <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 23 jul. 2020.

<sup>161</sup>*ibidem*, p. 8.

<sup>162</sup>*ibidem*.

Não bastasse, a ausência de garantias de tratamento adequado e seguro dos dados compartilhados parece-me agravada pela circunstância de que, embora aprovada, ainda não está em vigor a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais.<sup>163</sup>

Consta, também, no fundamento do referido *decisum*, as seguintes situações tendentes à violação de preceitos constitucionais fundamentais garantidores do direito à privacidade e da proteção de dados pessoais: (i) ausência de delimitação do objeto da pesquisa estatística; (ii) ausência de finalidade específica da utilização dos dados; (iii) falta de delimitação da amplitude necessária ao tratamento dos dados; (iv) inexistência de esclarecimentos sobre a “necessidade de disponibilização dos dados nem [sobre] como serão efetivamente utilizados”; e (v) carência de previsão de “mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento”<sup>164</sup>

Os ministros que acompanharam o voto da relatora fundamentaram a necessidade de suspensão da MP 954/2020, na medida em que, nos termos em que editado, o aludido instrumento normativo questionado viola preceitos fundamentais da Constituição Federal relativos à privacidade, à intimidade e ao sigilo de dados pessoais. Destacou-se, além disso, o dever de observância dos princípios da razoabilidade e da proporcionalidade diante de situações que relativizem as referidas garantias constitucionais.<sup>165</sup>

O ministro Gilmar Mendes, inclusive, fez oportuna menção ao acervo regulatório oriundo da Organização Mundial da Saúde (OMS) acerca da pandemia do coronavírus, o qual foi:

[...] incorporado ao ordenamento jurídico brasileiro por meio do Decreto 10.212/2020, [que] afasta a possibilidade de processamentos de dados desnecessários e incompatíveis com o propósito de avaliação e manejo dos riscos à saúde.<sup>166</sup>

Um ponto perceptível no julgamento em tela é o fato de o debate e a declaração dos votos dos ministros do STF estarem permeados pela temática do direito à proteção dos dados

<sup>163</sup> *ibidem*, p. 11.

<sup>164</sup> *ibidem*, p. 10.

<sup>165</sup> BRASIL. Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Brasília, DF: **Portal STF**, Notícias STF, 07 maio 2020. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>.

<sup>166</sup> *ibidem*.

personais, o que evidencia a maturação de um entendimento da Corte Constitucional brasileira favorável à autonomia de um direito fundamental à proteção dos dados pessoais.<sup>167</sup>

Terminada esta análise abrangente sobre os fundamentos normativos, objetivos e rol de direitos e definições previstos pela Lei Geral de Proteção de Dados brasileira, o capítulo a seguir pretende explicitar os mecanismos de tutela dos direitos dos titulares dos dados nas hipóteses de decisões automatizadas.

---

<sup>167</sup>AFFONSO, C. Discussão do STF sobre envio de dados ao IBGE foi de "1984" a fake News. **Tecfront**, Tilt, UOL, 07 maio 2020. Disponível em: <https://tecfront.blogosfera.uol.com.br/2020/05/07/discussao-do-stf-sobre-envio-de-telefones-ao-ibge-foi-de-1984-a-fake-news/>. Acesso em: 23.07.2020.

## 4 MECANISMOS DE TUTELA DOS DIREITOS DOS TITULARES DOS DADOS PESSOAIS DIANTE DAS DECISÕES AUTOMATIZADAS

Após a pavimentação do terreno teórico e normativo acerca do direito à proteção dos dados pessoais, o presente capítulo – cerne deste trabalho – propõe-se, de maneira clara e objetiva, a dissertar sobre os mecanismos de tutela dos direitos dos titulares dos dados pessoais diante de decisões tomadas por meios predominantemente ou exclusivamente automatizados.

### 4.1 Decisões automatizadas e riscos inerentes ao tratamento de dados pessoais por algoritmos

#### 4.1.1 *Big Data*, algoritmos e decisões automatizadas

Yuval Noah Harari, no final de seu livro *Homo Deus: A Brief History of Tomorrow*, trata do que ele denominou de “Religião dos Dados” (*The Data Religion*) ou “Dataísmo” (*Dataism*). Para Harari, o dataísmo seria uma espécie de religião e/ou concepção de mundo segundo a qual “o universo consiste em fluxo de dados, e o valor de qualquer fenômeno ou entidade é determinado pela sua contribuição para o processamento de dados”.<sup>168</sup>

O autor explicita que o dataísmo teria nascido de dois grandes paradigmas científicos: (i) o inaugurado há aproximadamente um século e meio pela obra *A Origem das Espécies* de Charles Darwin, a partir da qual “as ciências da natureza passaram a enxergar os organismos como algoritmos bioquímicos”; e (ii) a concepção, realizada cerca de oito décadas atrás, da Máquina de Turing de Alan Turing, e desde então “cientistas da computação têm aprendido a projetar algoritmos eletrônicos para vez mais sofisticados”.<sup>169</sup>

O dataísmo, assim, aproveita essas duas concepções, apontando que exatamente as mesmas leis matemáticas são aplicáveis a ambos os algoritmos (os bioquímicos e os eletrônicos), fazendo com que seja rompida a barreira entre animais e máquinas, à espera de que “os algoritmos eletrônicos eventualmente decifrem e superem os algoritmos bioquímicos”.<sup>170</sup>

---

<sup>168</sup>HARARI, Y. N. **Homo Deus**: A Brief History of Tomorrow. London: Vintage, 2017, p. 428, tradução nossa.

<sup>169</sup>*ibidem*.

<sup>170</sup>*ibidem*.

Sobre o ceticismo dos “dataístas” e sua fé inabalável do universo do fluxo de dados e das análises preditivas, Harari destaca que:

O Dataísmo inverte a pirâmide tradicional da aprendizagem. Até agora, os dados eram vistos apenas como o primeiro passo de uma longa corrente de atividade intelectual. Supunha-se que os humanos pudessem refinar dado em informação, informação em conhecimento e conhecimento em sabedoria. No entanto, os dataístas acreditam que os humanos não são mais capazes de lidar com o imenso fluxo de dados, o que, por consequência, retira a sua capacidade de transformar dado em informação, muito menos conhecimento em sabedoria. O trabalho de processamento de dado deveria, então, ser confiado a algoritmos eletrônicos, cuja capacidade em muito excede a do cérebro humano. **Na prática, dataístas são céticos acerca do conhecimento e sabedoria humanos, preferindo depositar sua confiança no Big Data e nos algoritmos computacionais.** [grifo nosso]<sup>171</sup>

Antes de se abordar a temática sobre *Big Data*, é oportuno tecer algumas observações sobre os chamados bancos de dados, os quais, de acordo com Doneda, são essencialmente “um conjunto de informações estruturado de acordo com uma determinada lógica [que] procura refletir um caráter utilitarista, procurando proporcionar a extração do máximo proveito possível a partir de um conjunto de informações. [...]”. Nesse sentido, “a novidade fundamental introduzida pelos computadores é a transformação de informação dispersa em informação organizada [Rodotà]”.<sup>172</sup>

Nesse contexto, um ponto fulcral abordado por Doneda diz respeito a “uma nova definição dos poderes e direitos sobre as informações pessoais, e conseqüentemente, sobre a própria pessoa”, resultado da elevada potência dos instrumentos tecnológicos de coleta, armazenamento e difusão de dados, bem como o crescente:

[...] número de sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estatuto jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo.<sup>173</sup>

Já o *Big Data*, segundo Bioni, é uma tecnologia que permite “que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades”, sendo “comumente associado a 3 (três) ‘Vs’: volume, velocidade e variedade [Doug Laney]”.

<sup>171</sup> *ibidem*, p. 429, tradução nossa.

<sup>172</sup> DONEDA, D. O direito fundamental à proteção de dados pessoais. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.<sup>a</sup> ed. Indaiatuba: Editora Foco, 2019, p. 39.

<sup>173</sup> *ibidem*.

O gigantesco progresso no volume de processamento de dados viabilizou a análise dos dados de modo abrangente, “tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles relações para desvendar padrões e, por conseguinte, inferir, inclusive, probabilidades de acontecimentos futuros.” Desse modo:

[t]orna-se possível, por exemplo, inferir a probabilidade de que uma consumidora esteja grávida, verificando-se que uma determinada lista de produtos é recorrentemente adquirida por tal tipo de cliente. É por meio dessa (cor)relação estabelecida entre fatos que se revela um padrão, ou seja, a recorrência de um evento que permite prever que eles se repetirão no futuro.<sup>174</sup>

Ao abordar a temática dos algoritmos, Maja Brkan atesta que não há definição comum sobre a noção de algoritmo na literatura. No entanto, a autora destaca que, em se tratando de processo decisório automatizado (*automated decision-making*), “estamos lidando com algoritmos computacionais que podem ser definidos como uma ‘sequência de passos para o cumprimento de uma tarefa que esteja descrita de forma precisa o suficiente para que um computador consiga realizá-la’”.<sup>175</sup>

Uma decisão automatizada, por sua vez, poderia ser definida simplesmente como a tomada de uma decisão sem a intervenção humana.<sup>176</sup> Para esta definição, Brkan apoiou-se nos dizeres do artigo 22 (1) do *General Data Protection Regulation* (GDPR), segundo o qual uma decisão individual automatizada é aquela que se baseia somente em um meio de processamento automatizado.

Parece ser esse o sentido atribuído pela Lei Geral de Proteção de Dados ao se referir, em seu art. 20, *caput*, ao direito do titular dos dados de requerer a revisão de “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais”.

Ana Frazão evidencia um cenário em que os algoritmos têm substituído cada vez mais as decisões humanas, “não apenas para dar respostas a questões objetivas, mas também para decidir questões subjetivas, complexas e que envolvem juízos sofisticados de valor”, tomando

<sup>174</sup>BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2018, p. 57-58.

<sup>175</sup>BRKAN, M. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. **International Journal of Law and Information Technology**, 11 jan. 2019. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3124901](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901). Acesso em: 20 out. 2019, p. 4, tradução nossa.

<sup>176</sup>*ibidem*.

por base os dados coletados no contexto do *Big Data*. Cita como exemplos os processos seletivos para preenchimento de cargos, definição de tipos de contratos a serem celebrados e a análise preditiva sobre a probabilidade de reincidência de um criminoso.<sup>177</sup>

Prossegue abordando conceitos como o *Machine learning*, que basicamente é a ideia de que os algoritmos podem “‘aprender’ e modificar sua própria estrutura e conduta, sem que haja propriamente controle ou mesmo previsibilidade sobre tais alterações e os resultados que daí decorrerão”.<sup>178</sup>

Essa característica de ausência de controle ou de previsibilidade sobre os resultados da operação de tratamento de dados pessoais é chamada pela literatura especializada de “opacidade algorítmica”. Na visão de Vedder e Naudts:

[...] **trade secrets** [are] among the main causes of **opacity of algorithms**, together with what he refers to as **technical illiteracy**, and **opacity that arises from the characteristics of machine learning and the scale required to apply them usefully** (Burrell 2016). Of course, ownership is different from the other factors of complication. It is not so much an intellectual difficulty, but rather an impediment for understanding. Without having access to the algorithm, or the context in which the algorithm is deployed, it is difficult to assess whether or not algorithmic decision-making is desirable in a given situation. Yet the decision to maintain algorithmic secrecy is, other than technical or contextual complexity, a man-made decision, and thus not inherent to the functioning of algorithms. [grifo nosso]<sup>179</sup>

Nesse sentido, Kamarinou e outros, destacando alguns aspectos técnicos a respeito da opacidade algorítmica, afirmam que alguns algoritmos baseados em *machine learning* “são mais favoráveis em permitir os humanos a detectar a maneira como eles – os algoritmos – operam; todavia, outros podem funcionar como uma espécie de ‘caixa-preta’ (*black box*)” [tradução nossa], conforme se trate ou não de sistemas algorítmicos que empregam complexas redes neurais em seu funcionamento, a exemplo de algoritmos de *deep learning*, o que, em termos práticos, inviabiliza o mapeamento do caminho adotado para se alcançar determinado resultado.<sup>180</sup>

<sup>177</sup> FRAZÃO, A. Algoritmos e inteligência artificial: Repercussões de sua utilização sobre a responsabilidade civil e punitiva das empresas. *Jota*, 15 maio 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018>. Acesso em: 05 jun. 2019.

<sup>178</sup> *ibidem*.

<sup>179</sup> VEDDER, A; NAUDTS, L. Accountability for the use of algorithms in a big data environment. *International Review of Law, Computers & Technology*, v. 31, Issue 2, p. 206-224, 08 mar. 2017, p. 5.

<sup>180</sup> KAMARINOU, D.; MILLARD, C.; SINGH, J. Machine Learning with Personal Data. *Legal Studies Research Paper* 247/2016. Queen Mary University of London, 2016. Disponível em: <https://ssrn.com/abstract=2865811>. Acesso em: 25 out. 2019, p. 19.

Ao dissertar sobre a proteção dos dados pessoais como forma de endereçar o problema da opacidade e da ausência de *accountability* da economia movida a dados, Ana Frazão denuncia que:

[...] os algoritmos podem perpetuar injustiças, preconceitos e discriminações. Em verdade, segundo John Kelleher e Brendan Tierney, como os algoritmos atuam de uma maneira mais amoral do que propriamente objetiva, quanto mais consistente for determinado preconceito em dada sociedade, mais forte será o padrão que aparecerá nos dados a respeito dessa sociedade e mais provável será que o algoritmo extraia e ainda replique esse padrão de preconceito.

**Por essa razão, John Gilliom e Torin Monahan destacam o fato de que tais sistemas, que são novas expressões de poder, fazem muito mais do que vigiar; efetivamente, trabalham para moldar nossas identidades e nos categorizar por meio de padrões sociais existentes e ainda vinculados a desigualdades de raça, classe e gênero para que, a partir daí, passemos a ser tratados diferentemente e a ter nossas escolhas e comportamentos alterados mediante premiações e punições.**

No mesmo sentido, Bruce Schneier ressalta a consolidação de um controle institucional, com parceria entre companhias e governos. Como muito dos dados são coletados e usados em segredo, as pessoas não podem refutar ou mesmo saber as evidências que são usadas contra elas, com o que se inibe o dissenso e a mudança social e ainda se abre margem para enorme potencial de manipulação. [...] [grifo nosso]<sup>181</sup>

Num cenário devastador como esse, o surgimento de instrumentos jurídicos que permitam a adequada e proporcional tutela do direito à privacidade e à proteção dos dados pessoais revela-se crucial, atuando como condição de possibilidade para o exercício de muitos outros direitos e liberdades.

Na subseção a seguir, serão feitos alguns apontamentos sobre os aspectos regulatórios do tratamento de dados pessoais.

#### 4.1.2 Base legal para o tratamento de dados pessoais

Uma concepção que vem sendo amplamente difundida a respeito da temática dos dados pessoais, conforme já abordado no subcapítulo 1.2 deste trabalho, é que estes, no contexto atual das sociedades da informação, atuam como uma espécie de combustível da economia, a

---

<sup>181</sup>FRAZÃO, A. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei geral de Proteção de Dados. In: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 39-40.

ponto de já se ter dito que o dado pessoal é o “novo petróleo” da Internet e a “nova moeda” do mundo digital.

Ressalta-se que é a partir da análise e tratamento de tais dados que os algoritmos conseguem transformá-los em informações que, por um lado, sejam úteis do ponto de vista econômico, mas que, por outro lado, podem gerar consequências prejudiciais aos direitos fundamentais dos usuários titulares dos dados.

Desse modo, um ponto primordial sobre o qual se concentram muitas pesquisas (nacionais e estrangeiras) são os aspectos jurídicos envolvendo o tratamento de dados pessoais, o qual é, justamente, a razão de ser da promulgação da Lei Geral de Proteção de Dados, na medida em que, conforme dispõe o art. 1º, o referido diploma legal é responsável por traçar as disposições gerais sobre o tratamento de dados pessoais em meios físicos ou 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”.

Nesse diapasão, a LGPD estabelece o conceito legal de tratamento de dados em seu art. 5º, inciso X, o qual vem a ser:

[...] **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. [grifo nosso]<sup>182</sup>

No que tange aos princípios a serem observados quando do tratamento de dados pessoais, a LGPD, em seu art. 6º, enumera dez incisos. Destacando-se apenas alguns deles, tem-se, primordialmente: a) o princípio da finalidade (“realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”); b) da transparência (“garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos

---

<sup>182</sup> BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (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: 20 jul. 2020.

comercial e industrial”); c) da prevenção (“adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais”) e; d) da não discriminação (“impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”).<sup>183</sup>

A Lei Geral de Proteção de Dados pátria, em seu artigo 5º, prescreve o conceito de dado pessoal como sendo “informação relacionada a pessoa natural identificada ou identificável” e dado pessoal sensível como aquele “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”.

De acordo com Doneda e Cunha, o tratamento automatizado de informações pessoais “suscitou o desenvolvimento de institutos jurídicos que procurassem oferecer meios efetivos de tutela da privacidade e garantir o direito à autodeterminação de cada pessoa em relação às próprias informações pessoais”.<sup>184</sup>

Na visão de tais autores, o surgimento de princípios informadores do tratamento de dados pessoais deriva da necessidade que existe em garantir o equilíbrio de interesses entre dois polos distintos:

[...] de um lado, a proteção do indivíduo e da sua privacidade na Sociedade da Informação e, de outro, a necessidade de estabelecer um patamar de licitude para que os vários serviços que fazem uso de dados pessoais possam operar com maior eficácia, respeitados os direitos individuais.<sup>185</sup>

Ocorre que, da simples análise da topologia da LGPD, bem como tendo em vista o contexto que tornou mais célere a sua promulgação no ordenamento jurídico brasileiro (com muitos casos amplamente noticiados de vazamento de dados pessoais), a edição do referimento diploma legal brasileiro teve como um de seus propósitos principais instituir

---

<sup>183</sup> *ibidem*.

<sup>184</sup> DONEDA, D.; CUNHA, M. V. A. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. Revista Brasileira de Risco e Seguro, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010, p. 89. Disponível em: <http://www.rbrs.com.br/arquivos/RBRS10-4%20Danilo%20Doneda.pdf>. Acesso em: 05 jun. 2019.

<sup>185</sup> *ibidem*.

mecanismos para coibir a coleta e o tratamento de dados pessoais de modo ilícito, muitas vezes sem a autorização ou ciência do titular de tais dados.

E, justamente para criar um sistema protetivo dos direitos dos titulares dos dados, o legislador, além de enunciar direitos e remédios voltados à efetividade da tutela do direito à proteção de dados pessoais, também destinou um capítulo específico para regular o tratamento de tais dados (Capítulo II – Do Tratamento de Dados Pessoais).

Com isso, merece menção o art. 7º da LGPD, no qual se prescrevem os requisitos que devem ser cumpridos quando qualquer sujeito realizar tratamento de dados pessoais, *in verbis*:

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

I - mediante o fornecimento de **consentimento pelo titular**;

II - para o **cumprimento de obrigação legal ou regulatória pelo controlador**;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à **execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a **realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, **a pedido do titular dos dados**;

VI - para o **exercício regular de direitos** em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a **proteção da vida ou da incolumidade física** do titular ou de terceiro;

VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos **interesses legítimos do controlador ou de terceiro**, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a **proteção do crédito**, inclusive quanto ao disposto na legislação pertinente. [...] [grifo nosso]

Importante sublinhar alguns elementos que assumem um papel de relevo em meio aos requisitos e à própria licitude e legitimidade do tratamento de dados pessoais. O consentimento é um deles, o qual “deve ser livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico”.<sup>186</sup>

A expressão “consentimento” surge 35 vezes ao longo da LGPD, o que inegavelmente denota a preocupação do legislador ordinário em colocar o titular dos dados numa posição

<sup>186</sup>BIONI, B. R., *op. cit.*, p. 188.

jurídica diferenciada, permitindo que ele tenha um papel importante no controle do fluxo de suas próprias informações, cumprindo com o postulado da autodeterminação informativa.<sup>187</sup>

A LGPD estabelece a obrigatoriedade de que, em se tratando de caso em que a base legal para o tratamento seja o consentimento do titular (art. 7º, I), o consentimento seja “fornecido por escrito ou por outro meio que demonstre a manifestação do titular” (art. 8º, *caput*), sendo “vedado o tratamento de dados pessoais mediante vício de consentimento” (art. 8º, §3º).

Outra base legal para o tratamento de dados bastante invocada por parte de quem realiza a atividade de tratamento é o legítimo interesse do controlador ou de terceiro (art. 7º, IX). Bioni aponta que o legítimo interesse está atrelado a uma ideia, transparecida pela própria LGPD, de “balanceamento entre a promoção das atividades do controlador e os direitos e liberdades fundamentais do titular”.<sup>188</sup>

Nesse sentido, o art. 10 da Lei Geral de Proteção de Dados dispõe sobre hipóteses (apenas exemplificativas) em que será considerado legítimo o interesse do controlador em realizar o tratamento de dados pessoais, *in verbis*:

Art. 10. O **legítimo interesse** do controlador somente poderá fundamentar tratamento de dados pessoais para **finalidades legítimas, consideradas a partir de situações concretas**, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os **dados pessoais estritamente necessários para a finalidade pretendida** poderão ser tratados.

§ 2º O controlador deverá adotar **medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse**.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. [grifo nosso]

Dessa maneira, considerando os supracitados regramentos em torno do legítimo interesse, Bioni afirma que o emprego dessa base legal para fins de tratamento de dados impõe que seja realizado (e devidamente documentado) um *teste de proporcionalidade*, consistente no(a): (i) “[v]erificação da legitimidade do interesse: situação concreta e

<sup>187</sup>*ibidem*.

<sup>188</sup>*ibidem*, p. 327.

finalidade legítima (art. 10, caput e I, da LGPD)”; (ii) “[n]ecessidade: minimização e outras bases legais (art. 10, § 1º, da LGPD)”; (iii) “[b]alanceamento: impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD)”; (iv) salvaguarda da “transparência e minimização dos riscos ao titular do dado (art. 10, §§ 2º e 3º, da LGPD)”.<sup>189</sup>

Além disso, da análise do art. 7º da LGPD, constata-se que há muitas outras bases legais que revestem de legitimidade e legalidade o tratamento de dados pessoais. Se um órgão do governo federal, por exemplo, mantém um cadastro e compartilha com outros órgãos de sua alçada dados pessoais de beneficiários de algum programa de transferência de renda, está-se diante de uma situação de tratamento de dados revestido de licitude, eis que destinado à execução de uma política pública (art. 7º, III). Se, por outro lado, em determinada situação concreta um órgão ou entidade de pesquisa, a exemplo do IBGE, utiliza dados pessoais para viabilizar seus estudos e pesquisas relativos, por exemplo, à renda média familiar *per capita* dos brasileiros, estar-se-ia diante de uma hipótese permitida por lei (art. 7º, IV).

Feitas essas considerações acerca das bases legais para tratamento de dados pessoais no contexto da Lei Geral de Proteção de Dados, a seguir serão expostos alguns riscos associados ao tratamento indevido de dados pessoais.

#### 4.1.3 Riscos associados ao tratamento indevido de dados pessoais

Sob a ótica de Monteiro, as leis que dispõem sobre a proteção de dados seriam como “‘guarda-chuvas’ regulatórios que protegem outros direitos”, uma vez que o âmbito de proteção da LGPD, por exemplo, não se restringiria apenas à tutela jurídica da privacidade, mas, em boa medida, se presta a resguardar outros direitos fundamentais e liberdades individuais “que somente podem ser exercidos na sua completude caso seja garantido o uso adequado dos dados pessoais que, muitas vezes, funcionam como representação do indivíduo”.<sup>190</sup>

---

<sup>189</sup>BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2018, p. 327 e ss.

<sup>190</sup>MONTEIRO, R. L. Artigo Estratégico 39: Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. Rio de Janeiro, dez. 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 05 jun. 2019, p.2.

O ponto-chave ressaltado por Monteiro é a falta de transparência acerca do funcionamento das decisões automatizadas (baseadas no uso de algoritmos) e os impactos que estas geram na vida das pessoas. Essa falta de transparência, segundo observa o autor, dificulta que sejam reconhecidas práticas discriminatórias, abusivas ou a caracterização de monopólios. A opacidade no tratamento de dados pessoais “impede que seus titulares tenham total compreensão de como seus direitos são impactados”.<sup>191</sup>

Assim, para ilustrar o impacto causado pelas decisões automatizadas em diferentes situações ensejadoras de autênticas violações ou restrições ao acesso a uma gama de direitos fundamentais, o supracitado autor relata exemplos envolvendo o direito à saúde, à educação, o direito ao pleno emprego, o direito à liberdade etc.

Segundo Ana Frazão:

[...] há hoje algoritmos que (i) identificam a orientação sexual da pessoa a partir do seu rosto; (ii) medem ondas cerebrais; (iii) reconhecem, a partir da análise cerebral, imagens vistas pelas pessoas, (iv) identificam estados emocionais, mentiras e intenções ocultas das pessoas; (v) reconhecem sinais de depressão, episódios de mania e outros distúrbios antes mesmo da manifestação de qualquer sintoma.<sup>192</sup>

Dentre as situações exemplificadas acima, talvez uma das mais impactantes diga respeito a uma situação envolvendo o direito à liberdade. A situação relatada trata de um caso real, ocorrido nos Estados Unidos da América, sobre um sistema computadorizado que calcula a pena a ser cumprida por um condenado a partir de uma base de dados que alimenta o sistema com informações sobre pena base, reincidência, bom comportamento, circunstâncias do crime praticado etc. O referido cálculo:

[...] geralmente é feito por um magistrado, que deve justificá-lo. Todavia, alguns sistemas jurídicos permitem a utilização de programas de computador para auxiliar no referido cálculo. (ANGWIN *et. al. apud* MONTEIRO, 2016) Tais sistemas, podem, ainda, comparar o caso com outros similares que estejam cadastrados em bases de dados públicas, e levar em consideração as peculiaridades das condenações anteriores para alimentar o algoritmo que irá auxiliar a atribuição da pena. **Assim, o algoritmo alimentado com dados pessoais dos condenados irá, por meio de um processo totalmente automatizado, determinar o tempo de encarceramento de um indivíduo.** [grifo nosso]<sup>193</sup>

<sup>191</sup>MONTEIRO, R. L., *op. cit.*, p.2-3.

<sup>192</sup>FRAZÃO, A. Algoritmos e inteligência artificial: Repercussões de sua utilização sobre a responsabilidade civil e punitiva das empresas. *Jota*, 15 maio 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018>. Acesso em: 05 jun. 2019.

<sup>193</sup>MONTEIRO, R. L., *op. cit.*, p.4.

Outro caso emblemático envolvendo o uso de algoritmos na esfera da responsabilização criminal é o caso de Brisha Borden, relatado no artigo de Julia Angwin e outros intitulado *Machine Bias*.<sup>194</sup>

Esse artigo revela que, na prática, os algoritmos computacionais podem acabar, de fato, incorporando padrões de análise baseados em preconceitos e concepções que promovem a discriminação entre os indivíduos. Isso porque Brisha, de 18 anos, foi classificada como sendo de elevado risco de reincidência delitiva (nota 8 de 10), a despeito de ter sido detida por tentar se apropriar de uma bicicleta para buscar a sua irmã na escola (em razão de seu atraso), além de outras pequenas infrações (“delitos juvenis”) de pequena monta cometidas no passado. Por outro lado, Vernon Prater, de 41 anos, foi detido por furtar itens de uma pequena loja de conveniência. Ele já havia sido condenado por roubo armado e tentativa de roubo armado, tendo recebido a pena de 5 anos de reclusão, além de ter sido acusado de outro roubo com emprego de arma. Entretanto, apesar desse histórico muito desfavorável, Vernon foi classificado pelo sistema algorítmico como sendo de baixo risco (nota 3 de 10).<sup>195</sup>

Tal discrepância apenas poderia ser explicada por um preconceito racial assimilado pelo algoritmo, na medida em que Brisha é negra e Vernon é branco, fato suficiente para haver a diferença de 5 pontos na escala de risco de reincidência delitiva. Assim, Angwin e outros demonstraram (inclusive apoiados em outros casos e em análises estatísticas) que o tratamento enviesado do algoritmo seguia o padrão de elevar a classificação de risco de pessoas negras apenas pelo fato de serem negras, o que revela um efeito perverso de uma decisão algorítmica e uma flagrante situação de violação ao princípio da dignidade da pessoa humana, à igualdade e à vedação à discriminação (interpretando tal situação à luz do ordenamento jurídico brasileiro).<sup>196</sup>

Nessa linha, Frazão assevera que, a partir da constatação de inúmeras situações lesivas aos direitos fundamentais das pessoas em casos de análises preditivas protagonizadas por sistemas baseados em algoritmos, é compreensível:

---

<sup>194</sup>ANGWIN, J. *et al.* Machine Bias. **ProPublica**, 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 05 jun. 2019.

<sup>195</sup>*ibidem*.

<sup>196</sup>*ibidem*.

[...] a farta literatura já existente a respeito dos riscos representados pelas decisões algorítmicas, inclusive no que se refere aos seus efeitos nefastos sobre as minorias e sobre os mais pobres, aumentando ainda mais a desigualdade. Cathy O’Neil chega a se referir aos algoritmos como armas matemáticas de destruição, na medida em que, longe de serem neutros e objetivos, embutem em seus códigos uma série de decisões e opiniões que não podem ser contestadas, até porque não são conhecidas. **Daí o seu potencial de destruição silenciosa, dado que podem basear seus julgamentos em preconceitos e padrões passados que automatizam o status quo e ainda podem ser utilizados para toda sorte de discriminações e violações de direitos.** [grifo nosso]<sup>197</sup>

Em seu artigo intitulado (numa tradução literal) “Contra Decisões Algorítmicas” (talvez uma tradução pertinente seja “Contra a Desumanização das Decisões”), Guido Noto La Diega, adotando um tom de manifesto, defende a impossibilidade de substituição de humanos por algoritmos, afirmando que “se deve começar a focar naquilo que nos torna humanos e a investir nossas energias em aprimorar e desenvolver habilidades e competências genuinamente humanas, como intuição e empatia”. [tradução nossa]<sup>198</sup>

O supracitado autor conclui, então, o seguinte:

Algorithms can and should be used as a form of artificial enhancement, to help judges and other decision-makers to find relevant sources and ensure consistency with precedents, but the law and decision-making are not a science that can be reduced to algorithmic processes. They are an art whose role will increasingly be understanding algorithmic decisions and being able to challenge them.<sup>199</sup>

Contra esse cenário de violação de direitos oriundo dos riscos do tratamento indevido de dados pessoais surge a necessidade da instituição e da efetiva execução de mecanismos que resguardem e promovam, de modo adequado, os direitos dos titulares dos dados pessoais. Alguns desses mecanismos serão sinteticamente abordados no próximo subcapítulo.

#### 4.2 Sistema remedial previsto pela Lei Geral de Proteção de Dados

<sup>197</sup>FRAZÃO, A. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei geral de Proteção de Dados. In: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 40.

<sup>198</sup>NOTO LA DIEGA, G. Against Algorithmic Decision-Making. **Northumbria Legal Studies Working Paper n. 2018/01**. University of Northumbria at Newcastle, 2018. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3135357](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135357). Acesso em: 20 out. 2019, p. 5-6.

<sup>199</sup>*ibidem*.

Conforme antecipado no subcapítulo 3.2 deste trabalho, Eduardo Souza e Rodrigo Silva realizam uma leitura dos artigos da Lei Geral de Proteção de Dados a partir de uma perspectiva remedial, isto é, reconhecem que, muito mais que *atribuir direitos*, a LGPD *enuncia verdadeiros remédios* voltados à tutela de direitos constantes do ordenamento jurídico brasileiro.

Nesse sentido, destacam os autores em tela que:

A preocupação com a disponibilização de meios de tutela dos direitos parece se refletir na tradicional formulação segundo a qual a ordem jurídica atribuiria ao titular do direito diversas medidas destinadas à sua conservação ou defesa. **A classificação dessas medidas variará de acordo com o critério de análise: quanto ao conteúdo, serão preventivas ou repressivas**, conforme visem, respectivamente, a evitar ou reprimir uma lesão; **quanto à forma de realização, serão judiciais ou extrajudiciais**, conforme dependam ou não, respectivamente, da intervenção judicial (AMARAL, 2008, p. 247). **O estudo dos chamados remédios, isto é, dos instrumentos voltados à tutela dos direitos, situa-se no âmago dessa discussão.** [grifo nosso] <sup>200</sup>

Souza e Silva ressaltam que os remédios em questão, na condição de instrumentos voltados à tutela dos direitos dos titulares dos dados, não podem ser concebidos como taxativos. Isso porque “um modelo rígido de taxatividade da tutela inibitória não se compatibiliza com o projeto constitucional de efetividade da tutela a ser dispensada aos direitos”. Assim, tem-se que o “**campo de abrangência das ações inibitórias há de ser tão amplo quanto a esfera de situações jurídicas subjetivas que venham a ser concretamente reputadas merecedoras de tutela**”. [grifo nosso] <sup>201</sup>

Sendo assim, a partir da adaptação da classificação acima transcrita (apenas no que tange ao *conteúdo* dos remédios), as seguintes subseções do presente trabalho monográfico terão o propósito de explicitar, sinteticamente, alguns mecanismos de **prevenção ou de limitação** e mecanismos de **repressão** à violação aos direitos fundamentais dos titulares dos dados.

#### 4.3 Mecanismos de prevenção ou de limitação à violação dos direitos fundamentais dos titulares dos dados

<sup>200</sup>SOUZA, E. N.; SILVA, R. G. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direito e a enunciação de remédios. **Pensar**, Fortaleza, v. 24, n. 3, p.1-22, jul./set. 2019, p. 3.

<sup>201</sup>*ibidem*, p. 14.

A Lei Geral de Proteção de Dados prevê uma série de mecanismos de prevenção ou de limitação à violação dos direitos fundamentais dos titulares dos dados de um modo geral.

Podem ser citados, em rol não exaustivo, o: (i) direito de correção de dados incompletos, inexatos ou desatualizados (art. 18, III); (ii) direito de acesso aos dados por seu titular (art. 18, I); (iii) o direito a solicitar a anonimização<sup>202</sup>, o bloqueio ou a eliminação de dados de titularidade do requerente (art. 18, IV); (iv) o direito de revogação do consentimento sobre o tratamento dos dados (art. 18, IX); (v) o direito à informação quanto à abrangência do compartilhamento dos dados (art. 18, VII); (vi) o direito à portabilidade dos dados a outros fornecedores de serviços ou produtos (art. 18, V).

É válido fazer a ressalva de que os mecanismos anteriormente abordados, de aplicação mais abrangente, também podem ser empregados para tutelar direitos em face de decisões automatizadas.

Apenas a título ilustrativo, seria plenamente possível que um titular dos dados exercesse o seu direito de correção de um dado desatualizado para remediar/combater uma decisão automatizada que, com base naquela informação que não mais subsiste, impediu o titular de ter acesso a algum bem, serviço ou a exercer algum direito ou prerrogativa que lhe fosse inerente.

O assim chamado direito ao esquecimento, de igual modo, a princípio seria perfeitamente aplicável a casos envolvendo tratamento de dados por meio de decisões automatizadas. Incidiria, neste caso, a figura do “right to erasure”. De acordo com Guilherme Martins, o “right to erasure”:

[...] é a vertente do direito ao esquecimento pela qual o próprio titular dos dados pode exigir que informações que lhe digam respeito sejam apagadas. Em outras palavras, o “right to erasure” consiste na simples remoção de dados pessoais fornecidos para tratamento automatizado.<sup>203</sup>

---

<sup>202</sup>Segundo a LGPD, a anonimização consiste na “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo” (art. 5º, XI).

<sup>203</sup> MARTINS, G. M. O direito ao esquecimento na internet. In: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.ª ed. Indaiatuba: Editora Foco, 2019, p. 80.

Nesse contexto, seria possível identificar na LGPD algumas referências ao direito ao esquecimento sob a forma de anonimização<sup>204</sup>, bloqueio ou eliminação de dados, a partir da leitura dos artigos 5º, III e XI e 18, IV e VI.

Já no que se refere especificamente aos mecanismos de prevenção ou de limitação à violação aos direitos dos titulares dos dados pessoais diante de decisões automatizadas, é possível extrair da LGPD um imperativo de transparência e *accountability* no contexto de processos decisórios baseados no uso de algoritmos.

Motivados pelas controvérsias geradas pelo caráter dual do tratamento de dados (utilidade econômica *versus* prejuízos aos direitos dos titulares dos dados) abarcadas pela própria Lei Geral de Proteção de Dados, faz-se válido analisar os trabalhos de Frazão<sup>205</sup> <sup>206</sup> e Monteiro<sup>207</sup>, os quais se preocupam em discorrer acerca dos denominados direitos à revisão e à explicação das decisões automatizadas de tratamento de dados pessoais.

Para instituir mecanismos jurídicos de constrangimento aos tipos de situações descritas principalmente na subseção 4.1.3 deste trabalho, a análise de Frazão é no sentido de que o art. 20 da Lei n. 13.709/2018 atua de modo a instituir “uma espécie de devido processo legal para proteger os cidadãos contra a ‘tirania’ dos julgamentos automatizados”, criando um “bloco de direitos” em favor do titular dos dados, abaixo transcrito:

- (i) o direito de acesso e informação a respeito dos critérios e procedimentos utilizados para a decisão automatizada, (ii) o direito de oposição quanto à decisão automatizada e de manifestar o seu ponto de vista, (iii) o direito de obtenção da revisão da decisão automatizada por uma pessoa natural e (iv) o direito de petição à

---

<sup>204</sup> Pela definição da LGPD, dado anonimizado é o “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (art. 5º, III).

<sup>205</sup> FRAZÃO, A. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Jota**, 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018>. Acesso em: 02 jun. 2019. Tecnologia.

<sup>206</sup> FRAZÃO, A. Data-driven economy e seus impactos sobre os direitos da personalidade: Indo além da privacidade e do controle dos dados pessoais. **Jota**, 17 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-17072018>. Acesso em: 02 jun. 2019. Tecnologia.

<sup>207</sup> MONTEIRO, R. L. Artigo Estratégico 39: Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. Rio de Janeiro, dez. 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 05 jun. 2019.

autoridade nacional para a realização de auditoria, em caso da não prestação das informações.<sup>208</sup>

Aqui é preciso fazer a ressalva da recente publicação da Lei nº 13.853/2019<sup>209</sup> oriunda do Projeto de Lei de Conversão Nº 7/2019 – proveniente, por sua vez, da Medida Provisória nº 869 de 2018 –, que promoveu mudanças em diversos artigos da Lei Geral de Proteção de Dados, especialmente naqueles que se referem à Autoridade Nacional de Proteção de Dados.

Todavia, interessa ao presente estudo, neste momento, apenas a alteração sofrida pelo art. 20 da LGPD, o qual passa a vigorar sem a previsão, antes expressa no *caput*, do direito subjetivo do titular dos dados de solicitar a revisão, **por pessoa natural**, das decisões automatizadas.

Em contrapartida, foram acrescentados os §§ 1º e 2º, os quais instituem a obrigatoriedade, por parte do controlador, de fornecer, em caso de requerimento pelo titular dos dados, informações “claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada”, resguardados os segredos comercial e industrial (§1º, art. 20). Nesta última hipótese (*trade secret*), a LGPD prevê que a ANPD (Autoridade Nacional de Proteção de Dados) poderá “realizar uma auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais” (§2º, art. 20).

Veja-se, na tabela a seguir, a nova redação do art. 20 da Lei Geral de Proteção de Dados na linha das alterações promovidas pela Lei nº 13.853/2019 [grifo nosso]:

**Tabela 3 – Quadro comparativo das alterações sofridas pelo artigo 20 da Lei n. 13.709/2018 (LGPD).**

Redação original	Art. 20. O titular dos dados tem direito a solicitar revisão, por pessoa natural, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o
------------------	---

<sup>208</sup>FRAZÃO, A. O direito à explicação e à oposição diante de decisões totalmente automatizadas. *Jota*, 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018>. Acesso em: 02 jun. 2019. Tecnologia.

<sup>209</sup>BRASIL. Lei 13.853 de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2019/Lei/L13853.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm). Acesso em: 24 nov. 2019.

	seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
Redação dada pela Medida Provisória nº 869 de 2018	<p>Art. 20. O titular dos dados tem direito a solicitar a revisão, <del>por pessoa natural</del>, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.</p> <p>§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.</p> <p>§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.</p> <p>§3º A revisão de que trata o caput deste artigo <b><u>deverá ser realizada por pessoa natural</u></b>, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados.</p>
Redação atual (Lei nº 13.853 de 2019)	<p>Art. 20 [...]</p> <p>§ 3º (VETADO)</p>

Fonte: Própria (2020).

Ao justificar as razões do veto ao §3º do art. 20 da LGPD (alterado pelo art. 2º do projeto de lei de conversão nº 7/2019, a Presidência da República, por meio da Mensagem nº 288, de 8 de junho de 2019, informou que, *ipsis litteris*:

A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.

Nota-se, portanto, que o Poder Executivo Federal agiu no sentido de favorecer o modelo de negócios das empresas que lidam com grande volume de transações e decisões automatizadas no desenvolvimento de suas atividades, priorizando-se o aspecto econômico em detrimento de um ganho nos aspectos de transparência e de garantia do exercício de outros direitos ligados ao regime de liberdades do indivíduo.

Prosseguindo-se com a análise dos artigos de Frazão e Monteiro, tem-se que, após os autores verificarem a existência de um **direito à explicação** (art. 20, §1º) e de um **direito à revisão ou oposição** (art. 20, *caput*), os autores chegam à conclusão de que os referidos direitos podem sofrer restrições à sua aplicação.

O direito à explicação tem o seu âmbito de aplicação reduzido pela necessidade expressa pelo §1º do art. 20 da LGPD de observância dos segredos comercial e industrial, bem como a dificuldade em superar a opacidade inerente aos sistemas algorítmicos complexos, a exemplo do *machine learning* e do *deep learning*, cujos próprios desenvolvedores são, muitas vezes, incapazes de averiguar a lógica por trás dos critérios de decisão tomados por sistemas inteiramente informatizados.<sup>210211</sup>

Por seu turno, tanto o direito à revisão (ou oposição) quanto o direito à explicação podem ter sua eficácia reduzida por questões de possível ausência de clareza ou falta de objetividade acerca de(o):

(i) o que vem a ser uma decisão totalmente automatizada, (ii) que tipos de decisão automatizada afetam a esfera jurídica dos titulares de dados e (iii) qual é o grau de transparência e explicação que será exigível em situações assim. Logo, é compreensível que existam muitas dificuldades interpretativas em torno desses direitos.<sup>212</sup>

A partir dos questionamentos supracitados, nota-se que, de fato, há a necessidade de um esclarecimento do conceito de “*decisões tomadas unicamente com base em tratamento automatizado de dados pessoais*”, tal como consta no art. 20, *caput*, da LGPD.

Isso porque seria possível pensar, por exemplo, em uma hipótese em que foi tomada uma decisão predominantemente realizada com base em tratamento automatizado de dados pessoais, e cuja eventual violação a um direito ou impedimento de exercício de um direito pelo titular dos dados tenha decorrido do processo decisório algorítmico (uma classificação indevida ou análise preditiva discriminatória), e não da etapa decisória a cargo de um humano. Nesse caso, pergunta-se: o titular dos dados seria tolhido de seu direito de solicitar a

---

<sup>210</sup>MONTEIRO, R. L., *op. cit.*, p.2.

<sup>211</sup>FRAZÃO, A. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Jota**, 05 dez. 2018a. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018>. Acesso em: 02 jun. 2019. Tecnologia.

<sup>212</sup>*idem*.

revisão de decisão? Se o critério de análise partir do próprio artigo 20 da LGPD, a resposta é incerta, o que revela uma espécie de lacuna deixada pelo legislador.

Outra constatação que se faz, a partir dos questionamentos feitos por Frazão e Monteiro, é a necessidade de maiores pesquisas a respeito de se e como seriam fornecidas “*informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada*” (Art. 20, §1º da LGPD), o que suscita a questão da viabilidade e da efetividade de um “direito à explicação”, considerando a barreira causada pela opacidade algorítmica e pelos segredos industrial e comercial, consoante aduzido anteriormente.

A despeito dessas indagações, o fato é que se afigura indiscutível a validade do direito à explicação e do direito à revisão de decisões automatizadas, cujas raízes remontam a três princípios informadores da LGPD: o princípio da finalidade (art. 5º, XII; art. 6º, I, II, III e V; art. 7º, §3º; art. 8º, §4º, e mais vinte referências), da transparência (art. 6º, VI; art. 9º, §1º; art. 10, § 2º; art. 40; art. 50, §2º, I, “e”) e da não-discriminação (art. 6º, IX).

Válido destacar, ainda, que Wachter, Mittelstadt e Floridi oferecem um contraponto à imposição do respeito ao segredo comercial e/ou industrial. Esse método alternativo de examinar – a despeito das barreiras técnicas, legais e organizacionais – a regularidade no tratamento de dados a cargo de decisões automatizadas consistiria na adoção de sistemas de auditoria externa (*a trusted third party*) com a finalidade de se proceder ao “exame de sistemas de decisão automatizada, incluindo a lógica e as circunstâncias de decisões específicas”. [tradução nossa]<sup>213</sup>

Essa abordagem, segundo os autores, possibilitaria ao controlador de dados a redução dos riscos relativos à exposição de segredos de negócio, ao mesmo tempo em que providenciaria um mecanismo de supervisão em favor dos titulares dos dados nos casos em que as explicações sejam inviáveis ou demasiadamente complexas para leigos.<sup>214</sup>

Além disso, conforme consta na **Tabela 3** elaborada anteriormente, o §2º do art. 20 da LGPD prevê que, caso o direito à explicação previsto pelo §1º do referido dispositivo seja

---

<sup>213</sup> WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 2017. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em: 20 out. 2019, p. 46.

<sup>214</sup> *ibidem*.

obstado pelo respeito ao segredo comercial e industrial, “a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais”.

A autoridade em questão é a Autoridade Nacional de Proteção de Dados – ANPD (atualmente com *status* de órgão integrante da Presidência da República, vide o art. 55-A, da LGPD), cuja estrutura, competências e demais disposições pertinentes estão contidas no Capítulo IX da Lei Geral de Proteção de Dados.

Assim, numa situação em que o titular dos dados se sinta prejudicado em razão da negativa à explicação, por motivos de segredo de negócio, acerca do processo decisório algorítmico que afetou algum interesse, o titular em questão pode peticionar administrativamente à ANPD, eis que assim lhe garante o §1º do art. 18 da LGPD ao estipular que o “titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional”.

Guido Noto La Diega menciona algumas hipóteses interessantes relativas a remédios contra decisões automatizadas. Dentre elas, é válido destacar uma, tendo em vista a sua aparente aplicabilidade à realidade brasileira.

O autor faz menção a um caso, ocorrido na Itália, em que uma organização sindical fez uso do direito à liberdade de informação “como uma ferramenta para acessar a lógica das decisões algorítmicas relativas à progressão de carreira de professores”. Todavia, o autor destaca que, na Europa, tal direito apenas pode ser invocado contra entes públicos.<sup>215</sup>

A princípio, seria possível admitir uma situação, no Brasil, em que um titular dos dados quisesse ter acesso à lógica por trás de um mecanismo de decisão automatizada implementado por algum órgão ou entidade pública, baseando-se na Lei de Acesso à Informação (LAI). A princípio, o titular conseguiria exercer a contento o seu direito de acesso à informação, desde que as informações por ele perseguidas não estivessem cobertas por sigilo em razão de risco à

---

<sup>215</sup> NOTO LA DIEGA, G. Against Algorithmic Decision-Making. **Northumbria Legal Studies Working Paper n. 2018/01**. University of Northumbria at Newcastle, 2018. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3135357](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135357). Acesso em: 20 out. 2019.

defesa e à soberania nacionais, risco à estabilidade econômica do país ou as demais hipóteses previstas pela LAI que versam sobre as exceções a direito de acesso à informação.

Existem, ainda, outras fórmulas e mecanismos de tutela dos direitos do titular dos dados pessoais que prezam pela concepção de sistemas de tratamento de dados mais responsáveis, compreensíveis e centrados no respeito aos direitos da personalidade.

Nesse sentido, Edwards e Veale, por demonstrarem ceticismo<sup>216</sup> com a existência e a efetividade de um direito à explicação em face de decisões algorítmicas no contexto europeu (chegando-se a utilizar a expressão “falácia da transparência”), propõem, a partir da perspectiva do GDPR, que há outros métodos tão ou mais eficazes que o aludido direito à explicação.<sup>217</sup>

São eles: (i) o *right to erasure*; (ii) o direito à portabilidade dos dados; (iii) *privacy by design*; (iv) relatórios de impacto à proteção dos dados pessoais (*Data Protection Impact Assessments*); e (v) selos de privacidade (*privacy seals*).<sup>218</sup>

O *right to erasure*, vertente do direito ao esquecimento, já foi abordado anteriormente, assim como o direito à portabilidade, valendo ressaltar que a LGPD abarca tais direitos.

Igualmente encontram previsão na LGPD disposições a respeito do relatório de impacto à proteção dos dados pessoais e dos selos de privacidade, conforme se vê a seguir:

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas [...]  
[...].§ 3º A autoridade nacional poderá solicitar ao controlador **relatório de impacto à proteção de dados pessoais**, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Art. 5º Para os fins desta Lei, considera-se:[...]  
XVII - **relatório de impacto à proteção de dados pessoais**: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; [...]

<sup>216</sup> Nas palavras dos autores: “Based on our analysis, we fear that the search for a “right to an explanation” in the GDPR may be at best distracting, and at worst nurture a new kind of “transparency fallacy.” (ibidem).

<sup>217</sup> EDWARDS, L.; VEALE, M. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions?”. **IEEE Security & Privacy**, maio/jun. 2018, p. 46-54. Disponível em: <https://arxiv.org/pdf/1803.07540.pdf>. Acesso em: 20 out. 2019, *passim*.

<sup>218</sup> *ibidem*.

Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de **relatórios de impacto à proteção de dados pessoais** e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: [...]

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:

- a) cláusulas contratuais específicas para determinada transferência;
  - b) cláusulas-padrão contratuais; [...]
  - c) normas corporativas globais;
  - d) **selos, certificados e códigos de conduta regularmente emitidos**; [...]
- [grifo nosso]

O conceito de *Privacy by design*, por sua vez, atrela-se à ideia de sistemas de informação que sejam projetados de uma maneira em que as normas protetivas de privacidade e de dados pessoais sejam automaticamente implementadas, fazendo com que as configurações padrão restrinjam o processamento de dados a um mínimo necessário.<sup>219</sup>

Há, inclusive, certo conjunto de estratégias vinculadas à concepção de *Privacy by Design*:

1. Minimizar – os dados coletados devem ser reduzidos ao mínimo possível;
2. Esconder – os dados e sua interrelação não devem ser publicizados;
3. Separar – o processamento dos dados deve se dar em compartimentos separados sempre que possível;
4. Agregar – os dados devem ser processados com alto nível de agregação e com o mínimo de detalhes;
5. Informar (transparência) – os sujeitos dos dados devem ser sempre informados dos processamentos de suas informações;
6. Controlar – os sujeitos dos dados devem ter controle sobre a coleta e o processamento de seus dados;
7. Fiscalizar e aplicar as leis – as políticas de privacidade devem estar em conexão com as exigências legais e devem poder ser fiscalizadas; e
8. Demonstrar – controladores de dados devem poder demonstrar o respeito às políticas de privacidade e aos requisitos legais.<sup>220</sup>

Por fim, para encerrar a abordagem acerca dos mecanismos de prevenção ou de limitação à violação dos direitos fundamentais dos titulares dos dados, é importante trazer à discussão as reflexões de Kamarinou, Millard e Singh.

<sup>219</sup>KOOPS, B. J. *et al. apud* VALENTE, J. Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy By Design e Privacy Enhancing Technologies. In: BRANCO, S.; TEFFÉ, C. (Org.). Privacidade em Perspectivas. Rio de Janeiro: Lumen Juris, 2018, p. 118.

<sup>220</sup>D'ACQUISTO, G. *et al. apud* VALENTE, J. Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy By Design e Privacy Enhancing Technologies. In: BRANCO, S.; TEFFÉ, C. (Org.). Privacidade em Perspectivas. Rio de Janeiro: Lumen Juris, 2018, p. 119.

As decisões automatizadas, de fato, podem gerar violações a direitos fundamentais dos titulares dos dados, na linha do que tem sido explicitado ao longo do presente trabalho. No entanto, é possível que as decisões automatizadas possam superar as limitações e os vieses presentes nas decisões humanas instituindo um processamento/tratamento potencialmente mais justo (“*fair processing*”), conforme se depreende do excerto abaixo:

*Whether a decision about us is being made by a human or by a machine, at present **the best we can hope for is that a decision that produces legal effects or significantly affects us will be as fair as humans can be.** An interesting possibility, however, is that **machines may soon be able to overcome certain key limitations of human decision makers and provide us with decisions that are demonstrably fair.** Indeed, it may already in some contexts make sense to replace the current model, whereby individuals can appeal to a human against a machine decision, with the reverse model whereby individuals would have a right to appeal to a machine against a decision made by a human.*[grifo nosso] <sup>221</sup>

Os autores em questão ressaltam que, relativamente ao “processamento justo” (*fair processing*), há que se ter em mente duas distinções conceituais.

Por um lado, existe a **discriminação como classificação e priorização da informação**, que, segundo Kamarinou e outros, “estão no coração do *machine learning*” [tradução nossa]. Por outro lado, há a **discriminação injusta**, a qual, num ambiente de *machine learning*, “pode ter origens em deficiências na qualidade e na quantidade dos dados disponíveis para treinar e testar o algoritmo, assim como em problemas com fontes, etiquetamento e preconceitos direta ou indiretamente infundidos em tais dados” [tradução nossa].<sup>222</sup>

Assim, para que tal patamar de *fair processing* seja alcançado, é preciso que a seguinte condição seja satisfeita: o algoritmo responsável pela tomada de decisões deve ter como base métodos de tratamento de dados e tecnologias que prezem pela transparência, *accountability*,

<sup>221</sup>KAMARINOU, D.; MILLARD, C.; SINGH, J. Machine Learning with Personal Data. **Legal Studies Research Paper 247/2016**. Queen Mary University of London, 2016. Disponível em: <https://ssrn.com/abstract=2865811>. Acesso em: 25 out. 2019, p. 22-23.

<sup>222</sup>*ibidem*.

observância aos direitos dos titulares dos dados e previsão de mecanismos de prevenção à discriminação (parâmetros éticos).<sup>223</sup>

Em suma, há de se respeitar os princípios atrelados à temática da proteção de dados pessoais, na medida em que, se tais princípios fossem realmente incorporados pelos sistemas de informação na ótica de padrões técnicos como o *privacy by design* e *privacy by default*<sup>224</sup>, muito pouco haveria de se discutir a respeito dos malefícios causados pelo emprego da tecnologia para tratamento de dados pessoais, especialmente se as práticas de boa governança<sup>225</sup> previstas e estimuladas pela Lei Geral de Proteção de Dados passassem a ser seguidas por todos os setores da sociedade responsáveis pelo tratamento de dados pessoais.

#### 4.4 Mecanismos de repressão à violação de direitos dos titulares por tratamento indevido de dados pessoais

Além dos instrumentos de prevenção ou limitação explicitados no subcapítulo anterior, a Lei Geral de Proteção de Dados também prevê uma série de mecanismos de repressão (ou sanção) ao tratamento de dados que resulte em violação aos direitos fundamentais dos titulares dos dados.

Na Seção III (Dos Agentes de Tratamento de Dados Pessoais) do Capítulo VI (Da Responsabilidade e do Ressarcimento de Dados), estão dispostos os artigos 42 a 45.

O art. 42 (*caput*) é claro ao imputar aos agentes de tratamento (isto é, ao controlador<sup>226</sup> ou ao operador<sup>227</sup>), relativamente ao exercício de atividade de tratamento de dados pessoais, a

<sup>223</sup> *ibidem*.

<sup>224</sup> Nesse sentido, cabe fazer alusão ao que dispõe o art. 51 da LGPD: “A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.”

<sup>225</sup> Acerca das práticas de boa governança, a LGPD dispõe o seguinte: “Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular **regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. [...]”

<sup>226</sup> Conforme define a LGPD, controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI).

**obrigação de reparar** o “dano patrimonial, moral, individual ou coletivo” decorrente da “violação à legislação de proteção de dados pessoais”. Ademais, admite-se o “direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso” (art. 42, §4º).

A responsabilidade do operador pelo tratamento dos dados que realiza é solidária na hipótese em que “descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador” (art. 42, I). Dentre essas obrigações, está incluído o dever de adotar as medidas de segurança previstas pela LGPD, haja vista que, em caso de omissão, os agentes de tratamento respondem pelo dano (art. 44, parágrafo único).

Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

A LGPD, relativamente ao tema de responsabilidade civil, admite expressamente que as “ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo [possam] ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente” (art. 42, §3º).

No que tange aos controladores, estes também respondem de forma solidária aos danos causados ao titular dos dados pessoais na situação em que eles – os controladores – estiverem diretamente envolvidos no tratamento (art. 42, II).

O art. 43 prevê, para algumas hipóteses excludentes da responsabilidade civil decorrente de danos causados ao titular dos dados, *in verbis*:

Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:  
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;  
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou  
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

---

<sup>227</sup> O operador, por sua vez, é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador” (art. 5º, VII).

O art. 44, por seu turno, delimita as situações que configuram tratamento irregular dos dados pessoais. Assim, o tratamento de dados realizados pelos agentes será tido como irregular “quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar” (art. 44, *caput*).

No contexto de tal tratamento, as seguintes circunstâncias deverão ser consideradas: “I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.”.

O art. 45, por sua vez, estabelece que os casos envolvendo violação do direito do titular no âmbito das relações consumeristas “permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”.

Logo, infere-se, a partir dessa delimitação normativa, que o Código de Defesa do Consumidor será amplamente utilizado como fundamento para reparação de danos que tenham sido causados pela irregularidade no tratamento de dados pessoais regidos pela Lei Geral de Proteção de Dados, mas cuja natureza contratual entre o titular e o responsável pelo tratamento seja classificada como relação de consumo.

Cabe destacar, entretanto, que, no tocante ao regime de responsabilidade civil aplicável aos agentes de tratamento, tem-se formado o entendimento, por parte de muitos autores, de que se trata, em regra, de **responsabilidade subjetiva**, a exigir, portanto, a caracterização dos requisitos do ato ilícito, dano, nexo causal e culpa. Isso porque:

Geralmente, o tratamento de dados não é uma atividade que traz graves riscos aos titulares, de forma que, não sendo hipótese de aplicação de alguma das teorias do risco – risco proveito ou risco criado – nem havendo expressa previsão de responsabilidade objetiva, a responsabilidade dos agentes de tratamento é, de fato, subjetiva.<sup>228</sup>

No entanto, a depender do caso concreto, o regime aplicável com relação aos agentes de tratamento de dados será o da **responsabilidade civil objetiva**, sem a necessidade de se pesquisar o elemento da culpa. Assim, a título de exemplo, em se tratando de relação de

---

<sup>228</sup> FERREIRA, D. R. Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva? **Jota**, 20 nov. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019>. Acesso em: 28 nov. 2019. Opinião & Análise, Dados pessoais.

consumo, “a violação à legislação de proteção de dados acarretará a aplicação dos institutos do fato do produto ou fato do serviço, sendo a reponsabilidade objetiva”,<sup>229</sup> na linha do que estipula o art. 45 da LGPD.

Ressalte-se que a imposição de um regime de responsabilidade objetiva também pode decorrer da teoria do risco criado “quando a atividade de tratamento, em razão da sua natureza ou elementos, apresentar graves riscos aos titulares”, a exemplo dos “incidentes de segurança envolvendo o tratamento de dados de crianças ou grupos vulneráveis, ou de pacientes de um hospital”.<sup>230</sup>

Nessa linha argumentativa, é interessante destacar o magistério de Caitlin Mulholland, a qual entende que

[...] **tanto o artigo 42, quanto o artigo 44, da LGPD, adotam o fundamento da responsabilidade civil objetiva**, impondo aos agentes de tratamento a obrigação de indenizar os danos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador. [grifo nosso]<sup>231</sup>

Segundo a autora, a adoção desse regime objetivo de responsabilidade civil com relação aos agentes de tratamento de dados tem como justificativa a natureza da atividade desenvolvida por esses sujeitos, bem como a natureza dos direitos passíveis de violação. É da natureza de tais atividades impor:

[...] riscos aos direitos dos titulares de dados, que, por sua vez, são intrínsecos, inerentes à própria atividade e resultam em danos a direito fundamental. Ademais, **tais danos se caracterizam por serem quantitativamente elevados e qualitativamente graves**, ao atingirem direitos difusos, o que, por si só, **já justificaria a adoção da responsabilidade civil objetiva, tal como no caso dos danos ambientais e dos danos causados por acidentes de consumo**. [grifo nosso]<sup>232</sup>

No mesmo sentido, Danilo Doneda e Laura Mendes sustentam que há riscos inerentes à atividade de tratamento de dados em si, sendo forçoso admitir, na linha do que se expôs ao longo deste trabalho, a “potencialidade danosa considerável em caso de violação desses

<sup>229</sup> *ibidem*.

<sup>230</sup> *ibidem*.

<sup>231</sup> MULHOLLAND, C. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?. **Migalhas**, 30 jun. 2020. Disponível em: <https://m.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpa-ou-risco>. Acesso em: 22 jul. 2020.

<sup>232</sup> *ibidem*.

direitos, que se caracterizam por sua natureza de direito personalíssimo e de direito fundamental”.<sup>233</sup>

Além disso, o escopo da LGPD traz consigo uma série de regras e princípios que limitam a atividade de tratamento de dados, a qual deve passar a atender aos postulados da necessidade, adequação, proporcionalidade, finalidade, dentre outros. Verifica-se, assim, que:

[e]stas considerações a respeito da finalidade da lei e dos princípios por ela adotados (necessidade, minimização, responsabilidade e prestação de contas, entre outros), levam os autores a concluir que o legislador optou por um regime de responsabilidade objetiva, vinculando o exercício da atividade de tratamento de dados pessoais a um risco inerente, potencialmente causador de danos a seus titulares.<sup>234</sup>

Dessa maneira, estando configurado o dano sofrido pelo titular dos dados decorrente de tratamento irregular pelos agentes responsáveis, é de se presumir que haverá a obrigação de reparação de danos de natureza patrimonial ou extrapatrimonial, na linha do que dispõe a própria LGPD e a cláusula geral de responsabilidade<sup>235</sup> oriunda do Código Civil.

O titular dos dados pessoais, portanto, estaria plenamente legitimado a lançar mão de ações judiciais com objetivo de impelir os responsáveis a repararem integralmente os danos, sejam eles morais ou patrimoniais – o que caracteriza tais vias ressarcitórias como **mecanismos repressivos** à violação dos direitos dos titulares dos dados.

Ao lado das ações de responsabilidade civil, há, igualmente, a possibilidade de o titular dos dados ajuizar ações que não veiculem pretensões indenizatórias, mas apenas pleiteiem o cumprimento de certa obrigação de fazer ou não fazer.

Assim, se o titular dos dados tiver a pretensão de fazer cessar algum tipo de violação decorrente do tratamento de dados pessoais – seja por órgão público ou entidade privada –, poderá, em tese, demandar judicialmente o cumprimento de alguma obrigação que não envolva o ressarcimento pelos danos causados, mas apenas a eliminação de seus dados pessoais de determinada base de dados, por exemplo.

---

<sup>233</sup>DONEDA, D.; MENDES, L. *apud* MULHOLLAND, C., *op. cit.*

<sup>234</sup>*ibidem.*

<sup>235</sup> Prescreve o art. 927 do Código Civil brasileiro que: “aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”.

Este seria um mecanismo de repressão mais brando, na medida em que, a princípio, não envolveria sanções pecuniárias em desfavor dos agentes de tratamento – ressalvada a hipótese de aplicação, pelo magistrado, de eventual multa por descumprimento de determinação judicial, bem como a provável condenação ao pagamento dos ônus de sucumbência.

Numa última análise, é válido discorrer brevemente sobre os mecanismos sancionatórios previstos pela Lei Geral de Proteção de Dados.

O art. 52 da LGPD estabelece que as violações às normas por ela previstas sujeitará os agentes de tratamento de dados a um rol de sanções administrativas, cuja aplicação ficará a cargo da autoridade nacional (ANPD).

Considerando-se apenas os incisos não vetados, as aludidas sanções são as seguintes:

- I - advertência, com indicação de prazo para adoção de medidas corretivas;
- II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III - multa diária, observado o limite total a que se refere o inciso II;
- IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI - eliminação dos dados pessoais a que se refere a infração;

Nota-se, com isso, a variedade de instrumentos de repressão dos quais dispõe a Autoridade Nacional de Proteção de Dados, a qual pode aplicar desde uma sanção mais branda como uma advertência (art. 52, I), até uma sanção que, por exemplo, abale significativamente a esfera patrimonial de uma sociedade empresária no caso de aplicação de multa que pode atingir cifras milionárias (art. 52, II).

Vale transcrever o que dispõe o §1º do art. 52, a respeito dos critérios de aplicação das sanções administrativas:

Art. 52. [...]

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, **de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:**

- I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- II - a boa-fé do infrator;
- III - a vantagem auferida ou pretendida pelo infrator;
- IV - a condição econômica do infrator;
- V - a reincidência;
- VI - o grau do dano;
- VII - a cooperação do infrator;
- VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
- IX - a adoção de política de boas práticas e governança;
- X - a pronta adoção de medidas corretivas; e
- XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. [...]  
[grifo nosso]

É digno de nota o fato de tais sanções estarem submetidas à possibilidade de aplicação gradativa, isolada ou, até mesmo, cumulativa, a partir de uma análise casuística a cargo da autoridade competente, a quem aparentemente a LGPD atribuiu uma esfera de discricionariedade no processo administrativo sancionador, desde que sejam atendimentos os parâmetros e critérios expressamente enumerados pela lei em comento.

Outro ponto a ser ressaltado é a questão atinente à aplicação de sanções administrativas em desfavor de entidades e órgãos públicos. Nesse caso, a sanção de multa não incidirá sobre os agentes integrantes do aparato estatal, conforme disposição expressa do art. 52, §3º, da LGPD.

Entretanto, este mesmo dispositivo legal prevê que as demais sanções de natureza não pecuniária (advertência com indicação de prazo para medidas corretivas, publicização da infração, bloqueio e eliminação dos dados pessoais) serão plenamente aplicáveis aos agentes públicos, os quais ainda poderão ser condenados pelas sanções previstas na Lei n. 8.112/1990, na Lei de Improbidade Administrativa (Lei n. 8.429/1992) e na Lei de Acesso à informação (Lei n. 12.527/2011).

Os artigos 53 e 54, por conseguinte, versam sobre o meio de definição das sanções e as metodologias a servirem de norte para a fixação do valor das multas administrativas e das multas diárias. Confirmam-se:

Art. 53. A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei, que deverá ser objeto de consulta pública, as metodologias que orientarão o cálculo do valor-base das sanções de multa.

§ 1º As metodologias a que se refere o caput deste artigo devem ser previamente publicadas, para ciência dos agentes de tratamento, e devem apresentar objetivamente as formas e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos nesta Lei.

§ 2º O regulamento de sanções e metodologias correspondentes deve estabelecer as circunstâncias e as condições para a adoção de multa simples ou diária.

Art. 54. O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado e ser fundamentado pela autoridade nacional.

Parágrafo único. A intimação da sanção de multa diária deverá conter, no mínimo, a descrição da obrigação imposta, o prazo razoável e estipulado pelo órgão para o seu cumprimento e o valor da multa diária a ser aplicada pelo seu descumprimento.

Por fim, é importante ressaltar que a efetividade dos mecanismos de tutela dos direitos do titular dos dados – tanto os instrumentos preventivos quanto os repressivos – dependerá, de modo considerável, de uma autoridade nacional que atue de modo firme e diligente em todas as frentes necessárias para a garantia do direito à proteção dos dados pessoais dos cidadãos, bem como dos direitos fundamentais a ele conexos.

## CONCLUSÃO

A edição de uma lei de proteção de dados de abrangência nacional era uma demanda apontada por muitos autores brasileiros que discorriam sobre o vácuo legislativo existente na temática da proteção de dados, na medida em que, ao longo das últimas décadas, o ordenamento infraconstitucional pátrio abrigava apenas leis setoriais que tutelavam alguns aspectos da proteção de dados pessoais limitados, naturalmente, à esfera de atuação das atividades específicas (ou seja, aos “setores”) que tais instrumentos normativos buscavam regular.

Com a publicação, em 2014, do Marco Civil da Internet (MCI – Lei n. 12.965/2014), o legislador ordinário deixou indícios da pretensão de futura edição de uma lei de tal natureza, pois o art. 3º, inciso III, do MCI, preconizou que a “disciplina do uso da internet no Brasil” tem como princípio, dentre outros, o da “proteção dos dados pessoais, *na forma da lei*”.

Em 2016, com o nascimento do Regulamento Geral de Proteção de Dados da União Europeia – GDPR, somado aos notórios casos internacionais (e transnacionais) de vazamento, manipulação e outros artifícios envolvendo dados pessoais de milhões de pessoas ao redor do globo, não havia mais volta: urgia que se editasse um marco de proteção de dados no Brasil.

Atendendo a essa demanda (antiga em muitos países, nos quais o debate sobre dados pessoais já atingia “outro patamar”), o Congresso Nacional aprovou, em 2018, a Lei Geral de Proteção de Dados (LGPD – Lei n. 13.709/2018), que, a partir de uma filtragem constitucional ressignificadora do direito à privacidade e à inviolabilidade das comunicações de dados, enunciou os direitos que constituem o objeto de estudo do presente trabalho.

Mais especificamente, este trabalho se propôs a dissertar sobre a LGPD e a tutela dos direitos do titular dos dados pessoais nas hipóteses envolvendo decisões automatizadas que gerem consequências negativas na esfera jurídica do titular.

Verificou-se em que medida os direitos, garantias e procedimentos previstos pela Lei Geral de Proteção de Dados tutelam adequadamente os direitos dos titulares dos dados nos casos de decisões tomadas por meios automatizados tendentes a violar um ou mais direitos fundamentais.

Ao longo de quatro capítulos, promoveu-se uma abordagem centrada na doutrina nacional e internacional acerca do tema do direito à proteção dos dados pessoais, além de uma análise sistemática dos dispositivos constitucionais e infraconstitucionais que sustentam a autonomia do direito em tela.

Inicialmente, procurou-se contextualizar o momento atual vivenciado pela sociedade, adotando como marco teórico os ensinamentos de Manuel Castells sobre o conceito de sociedade em rede e de Stefano Rodotà acerca da sociedade da vigilância e sociedade da classificação. Nesse tipo de sociedade, os dados assumem o papel de um valioso ativo econômico, constituindo a peça central de uma economia movida a dados, cuja coleta e tratamento se dão de modo generalizado e em grande volume, sendo comuns cenários de falta de consentimento ou desconhecimento dos titulares relativamente ao destino de seus dados pessoais.

A respeito das origens do direito à proteção de dados, viu-se que este se origina do direito à privacidade, o qual se caracteriza como um instituto multifacetado, pois seu núcleo conceitual sofreu (e ainda continua a sofrer) diversas modificações de sentido ao longo do tempo.

As faces do direito à privacidade vão desde o “direito a ser deixado em paz” ou do “direito a estar só” (marco comumente associado ao artigo *The right of privacy* de Samuel Warren e Louis Brandels, publicado no final do século XIX) até o “direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada” (como muito bem delineou Stefano Rodotà, em *A vida na sociedade da vigilância: A privacidade hoje*).

O desenvolvimento das tecnologias da informação e a densidade assumida pelo princípio da dignidade da pessoa humana (de que decorre o princípio do livre desenvolvimento da personalidade) fizeram com que a leitura normativa do direito à privacidade como respeito à vida privada e à intimidade já não fosse mais suficiente para tutelar os direitos de um indivíduo, advindo daí a nova função da privacidade: possibilidade de proteção e controle efetivos dos dados pessoais. Nas lentes de Rodotà, a estrutura conceitual e funcional do direito à privacidade passa a se concentrar no eixo “pessoa-

informação-circulação-controle” no lugar do paradigma clássico da “pessoa-informação-segreto”.

Percebeu-se, ainda, que essa nova roupagem do direito à privacidade acompanhou o movimento de constitucionalização do direito civil, marcado pelos traços de despatrimonialização e crescente realce da dignidade da pessoa humana, havendo o predomínio de situações jurídicas existenciais sobre as relações eminentemente patrimoniais.

Em seguida, o presente trabalho procurou demonstrar de que modo o direito à proteção dos dados pessoais pode ser concebido, ao mesmo tempo, como direito da personalidade e como direito fundamental à luz do ordenamento jurídico brasileiro.

A partir de uma convergência conceitual dos autores abordados, viu-se que os direitos da personalidade são aqueles relativos “à tutela da pessoa humana, considerados essenciais à sua dignidade e integridade”, segundo o magistério de Gustavo Tepedino. Referidos direitos da personalidade, pelos ensinamentos de Maria Celina Bodin de Moraes, também possuem um caráter não-exaustivo ou elástico, abrangendo um número ilimitado de hipóteses, tendo sempre como norte a cláusula geral de tutela da pessoa humana.

Nesse sentido, Bruno Bioni, por exemplo, corroborou o enquadramento do direito à proteção de dados como direito da personalidade, uma vez que, na sua concepção, um dado que revele algo de alguma pessoa pode ser atrelado aos direitos da personalidade desde que esteja presente a qualificação de “pessoal”, hipótese na qual um dado dessa natureza assume “uma projeção, extensão ou dimensão do seu titular”.

Assim, o âmbito normativo do direito à proteção dos dados pessoais passa a inibir possíveis situações discriminatórias e que impeçam, em menor ou maior grau, o livre desenvolvimento da personalidade e a autodeterminação informativa, bem como o exercício dos mais diversos direitos fundamentais.

Rodotà assinalou que, a partir dos “riscos conexos ao uso das informações coletadas”, desenvolveu-se a noção de autodeterminação informativa, cujo caráter de direito fundamental é reconhecido por diversos ordenamentos jurídicos.

Além de se constituir como um direito da personalidade, o direito à proteção de dados pessoais também se configura como um direito fundamental à luz dos princípios e regras adotados pela CRFB/1988, por razões que vão desde sua origem (“pressupostos ontológicos”, vide Danilo Doneda) comum ao direito à privacidade (art. 5º, X), passando pela tutela conferida ao fluxo informações presente no direito à inviolabilidade e ao sigilo das comunicações de dados (art. 5º, XII), até se chegar à análise da dignidade da pessoa humana (art. 1º, III) como fundamento normativo vinculado ao regime de proteção dos dados que se apresentam como extensão da personalidade.

Ressaltou-se, também, que tramita, desde 2019, uma Proposta de Emenda à Constituição (PEC) no Congresso Nacional que tem o objetivo de inserir, formalmente, o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais da Constituição da República Federativa do Brasil, representando uma cautela adicional do Poder Constituinte Reformador no sentido de assegurar a fundamentalidade formal do direito em questão.

De todo dado pessoal pode ser extraída uma informação de cunho público ou privado. Tal constatação gera a ruptura da dicotomia clássica entre a esfera pública e a esfera privada quando se está em jogo o direito à proteção de dados pessoais, pois este possui autonomia em relação ao direito à privacidade. A aludida autonomia foi, inclusive, reforçada pelo Plenário do Supremo Tribunal Federal, conforme detalhado no subcapítulo 3.4.

Seguindo essa linha argumentativa, é válido destacar que, indo ao encontro da preocupação central que originou o presente trabalho, Bioni realçou o impacto que o tratamento de dados causa na vida dos indivíduos, ainda mais em se tratando de processos decisórios algorítmicos “que irão definir seu próprio futuro”.

Exemplo disso foi a perplexidade que gerou o caso retratado por Julia Angwin e outros na subseção destinada a abordar, em caráter não exaustivo, os riscos associados ao tratamento indevido de dados pessoais (subseção 4.1.3). Numa situação envolvendo mecanismo automático de classificação de risco de periculosidade de indivíduos detidos pela prática de delitos, uma jovem negra com ficha criminal modesta foi classificada com grau 8 de 10, enquanto um homem branco de meia-idade com ficha extensa e marcada por crimes violentos recebeu o grau 3 de 10.

O caso em questão forneceu indícios robustos que levam a crer que, quando mal projetados, os sistemas algorítmicos incorporam em suas bases preconceitos e lógicas preditivas que levam a decisões evidentemente discriminatórias e prejudiciais a certos grupos.

A “opacidade algorítmica” (definida pela falta de controle ou de previsibilidade sobre os resultados da operação de tratamento de dados pessoais) e a complexidade inerente aos sistemas de *machine learning*, *deep learning* e assemelhados não podem representar um cheque em branco que expõe os cidadãos a toda sorte de agressões a direitos fundamentais. Ao menos não em um Estado Democrático de Direito permeado por princípios e paradigmas axiológicos próprios do Constitucionalismo Contemporâneo.

Há de se abrir, portanto, a “caixa-preta” que caracteriza tais sistemas algorítmicos. E o caminho para a superação dos efeitos colaterais indesejáveis de uma economia movida a dados é traçado, no que tange à realidade brasileira, pelos princípios e garantias previstas na Constituição Federal, assim como pelo arcabouço normativo previsto pela ordem infraconstitucional, especialmente aquele constante da Lei Geral de Proteção de Dados.

Forçoso reconhecer que a LGPD e a sua fonte inspiradora, o GDPR, instituem uma série de princípios, diretrizes, direitos, deveres, obrigações e procedimentos no sentido induzir as organizações que realizam costumeiramente o tratamento de dados pessoais a reforçar o “accountability algorítmico” e o controle de riscos.

É o que se observou no último capítulo deste trabalho, onde se discorreu sobre o prisma remedial previsto na LGPD, os mecanismos de prevenção, limitação e repressão à violação dos direitos dos titulares dos dados quando sujeitos a decisões tomadas por meios automatizados.

Os direitos atribuídos e a enunciação de remédios no bojo da LGPD não podem ser lidos de modo taxativo, isso porque, conforme acertada lição de Souza e Silva, o “campo de abrangência das ações inibitórias há de ser tão amplo quanto a esfera de situações jurídicas subjetivas que venham a ser concretamente reputadas merecedoras de tutela”.

Nesse sentido, procurou-se abordar, sempre em caráter exemplificativo, medidas que podem ser tomadas pelo titular dos dados para a efetiva tutela de seus direitos, tendo sido escolhida uma abordagem que leva em conta a classificação dessas medidas quanto ao conteúdo (preventivas ou repressivas).

Como medidas preventivas ou limitadoras à violação dos direitos do titular dos dados, explicitaram-se: (i) o direito de correção de dados incompletos, inexatos ou desatualizados (art. 18, III, da LGPD); (ii) direito de acesso aos dados por seu titular (art. 18, I); (iii) o direito a solicitar a anonimização, o bloqueio ou a eliminação de dados de titularidade do requerente (art. 18, IV); (iv) o direito de revogação do consentimento sobre o tratamento dos dados (art. 18, IX); (v) o direito à informação quanto à abrangência do compartilhamento dos dados (art. 18, VII); (vi) o direito à portabilidade dos dados a outros fornecedores de serviços ou produtos (art. 18, V).

Foi possível, outrossim, identificar na LGPD algumas referências ao direito ao esquecimento sob a forma de anonimização, bloqueio ou eliminação de dados, a partir da leitura dos artigos 5º, III e XI e 18, IV e VI.

Adentrando no mérito de mecanismos voltados preponderantemente aos imperativos de *accountability* e transparência nas decisões algorítmicas, observou-se que Frazão e Monteiro, por exemplo, reconheceram a existência de um direito à explicação (art. 20, §1º, da LGPD) e de um direito à revisão ou oposição (art. 20, *caput*, da LGPD), os quais, todavia, podem sofrer limitações fáticas (opacidade algorítmica) e barreiras normativas (segredos comerciais e industriais), fato que enfraquece sua capacidade de promover uma tutela efetiva da proteção dos dados pessoais e direitos conexos.

Uma solução possível seria aquela apontada por Wachter, Mittelstadt e Floridi, de acordo com os quais o controlador de dados poderia reduzir os riscos de exposição de segredos de negócio introduzindo a figura do auditor externo (*a trusted third party*). Esse sistema de auditoria seria responsável por prover um mecanismo de supervisão em favor dos titulares dos dados nos casos em que as explicações sejam inviáveis ou demasiadamente complexas para leigos.

Insta apontar que a própria LGPD aponta uma solução à controvérsia, desta vez instituindo um mecanismo de auditoria a cargo da Autoridade Nacional de Proteção de Dados – ANPD, a qual objetivará verificar “aspectos discriminatórios em tratamento automatizado de dados pessoais”.

Outras medidas igualmente eficazes, ainda na esfera que previne e limita violações de direitos, são o *right to erasure*; o direito à portabilidade dos dados; *privacy by design*; relatórios de impacto à proteção dos dados pessoais (*Data Protection Impact Assessments*) e os selos de privacidade (*privacy seals*) – muitos destes previstos pela Lei Geral de Proteção de Dados.

Como contraponto interessante à hipótese inicial deste trabalho monográfico (que apenas enxergava com desconfiança o sistema de decisões algorítmicas sem intervenção humana), é importante destacar as reflexões de Kamarinou, Millard e Singh. Tais autores visualizam um cenário onde as decisões automatizadas possam superar as limitações e os vieses presentes nas decisões humanas instituindo um processamento de dados potencialmente mais justo. A isto denominaram “*fair processing*”, cujo algoritmo responsável pela tomada de decisões deve se estruturar a partir de métodos de tratamento de dados e tecnologias que prezam pela transparência, *accountability*, observância aos direitos dos titulares dos dados e previsão de mecanismos de prevenção à discriminação (parâmetros éticos).

Noutro giro, no que diz respeito aos mecanismos repressivos, o titular dos dados pessoais, estaria plenamente legitimado a lançar mão de ações judiciais com objetivo de impelir os responsáveis a reparar integralmente os danos, sejam eles morais ou patrimoniais.

Além da via do ressarcimento do dano, há uma infinidade de medidas judiciais ou administrativas (a exemplo das sanções aplicadas pela ANPD, vide artigos 52 a 54 da LGPD) que tratam de constranger o agente de tratamento de dados a responder, de alguma forma, pela violação por ele causada, conforme exposto no presente trabalho.

Não se pode negar que o contexto brasileiro carece de uma entidade regulatória central responsável por conduzir políticas voltadas à tutela efetiva dos direitos dos titulares dos

dados, atuando como agente interlocutor entre os agentes de tratamento de dados e as pessoas naturais sujeitas ao *modus operandi* da sociedade informacional e de vigilância.

Por fim, é preciso dizer, todavia, que eternas prorrogações da *vacatio legis* dos dispositivos da LGPD não parecem ser a melhor solução para a realidade nacional. Isso porque, muito mais do que um mero carrasco do Direito Administrativo Sancionador que impõe medo por meio de pesadas multas, a ANPD deverá ter uma atuação pautada na prevenção de riscos e no estímulo à adequação normativa por parte dos inúmeros setores públicos e privados que lidam diariamente com tratamento de dados, promovendo-se uma variedade de mecanismos técnicos ou administrativos que busquem preservar a integridade dos dados, assegurando o seu tratamento apenas aos fins legítimos e lícitos a que se destinam.

## REFERÊNCIAS BIBLIOGRÁFICAS

AFFONSO, C. Discussão do STF sobre envio de dados ao IBGE foi de “1984” a fake news. **Tecfront**, Tilt, UOL, 07 maio 2020. Disponível em: <https://tecfront.blogosfera.uol.com.br/2020/05/07/discussao-do-stf-sobre-envio-de-telefones-ao-ibge-foi-de-1984-a-fake-news/>. Acesso em: 23.07.2020.

ANGWIN, J. et al. Machine Bias. **ProPublica**, 23 maio 2016. Disponível em: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Acesso em: 05 jun. 2019.

BAIÃO, K. S.; GONÇALVES, K. C. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilistica.com**. Rio de Janeiro, a. 3, n. 2, jul.-dez. 2014, p. 17. Disponível em: <http://civilistica.com/agarantia-da-privacidade-na-sociedade-tecnologica-um-imperativo-a-concretizacao-do-principio-dadignidade-da-pessoa-humana/>. Acesso em: 07 nov. 2019.

BARROSO, L. R. **A dignidade da pessoa humana no direito constitucional contemporâneo**: A construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Editora Fórum, 2014.

BIONI, B. R. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2018.

BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Elsevier, 2004.

BONAVIDES, P. **Curso de Direito Constitucional**. 33.<sup>a</sup> ed. São Paulo: Malheiros Editores, 2018.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2019]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 13 nov. 2019.

BRASIL. **Lei n. 3.071, de 1º de janeiro de 1916 [Código Civil de 1916]**. Código Civil dos Estados Unidos do Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/13071.htm](http://www.planalto.gov.br/ccivil_03/leis/13071.htm). Acesso em: 23 nov. 2019.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990 [Código de Defesa do Consumidor]**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da

República, 1990. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8078.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078.htm). Acesso em: 23 nov. 2019.

**BRASIL. Lei n. 10.406, de 10 de janeiro de 2002 [Código Civil de 2002].** Institui o Código Civil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm). Acesso em: 23 nov. 2019.

**BRASIL. Lei n. 12.414, de 9 de junho de 2011 [Lei do Cadastro Positivo].** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Brasília, DF: Presidência da República, 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112414.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112414.htm). Acesso em: 23 nov. 2019.

**BRASIL. Lei n. 12.527, de 18 de novembro de 2011 [Lei de Acesso à Informação].** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112527.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112527.htm). Acesso em: 23 nov. 2019.

**BRASIL. Lei n. 12.965, de 23 de abril de 2014 [Marco Civil da Internet].** 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/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 23 nov. 2019.

**BRASIL. Lei n. 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados (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: 9 jun. 2019.

**BRASIL. Lei 13.853 de 8 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2019-2022/2019/Lei/L13853.htm](http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm). Acesso em: 21 jul. 2020.

**BRASIL. Lei n. 14.010, de 10 de junho de 2020.** Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF: Presidência da República, 2020.

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/lei/L14010.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm). Acesso em 21 jul. 2020.

**BRASIL. Medida Provisória n. 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 21 jul. 2020.

**BRASIL. Medida Provisória n. 959, de 29 de abril de 2020.** Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD. Brasília, DF: Presidência da República, 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/mpv/mpv959.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm). Acesso em 21 jul. 2020.

**BRASIL. Ministério da Justiça. Escola Nacional de Defesa do Consumidor. A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. (Elaboração: Danilo Doneda). Brasília: SDE/DPDC, 2010, p. 29. Disponível em: <https://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protacao-de-dados-pessoais.pdf>. Acesso em: 01 set. 2019.

**BRASIL. Proposta de Emenda Constitucional 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. Brasília, DF: Senado Federal, 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 14 nov. 2019.

**BRASIL. Proposta de Emenda Constitucional nº 17, de 2019.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Câmara dos Deputados, 2019. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757>. Acesso em: 20 jul. 2020.

**BRASIL. Supremo Tribunal Federal. AÇÃO DIRETA DE INCONSTITUCIONALIDADE:** ADI n. 6387/DF – Distrito Federal. Ministra Relatora: Rosa Weber. Brasília, DF: **Portal STF**, Processos, Andamentos, 2020. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165>. Acesso em: 23 jul. 2020.

BRASIL. Supremo Tribunal Federal. AÇÃO DIRETA DE INCONSTITUCIONALIDADE: ADI n. 6387/DF – Distrito Federal. Ministra Relatora: Rosa Weber. Brasília, DF: **Portal STF**, Processos, Decisões, 2020.

<http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 23 jul. 2020.

BRASIL. Supremo Tribunal Federal. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Brasília, DF: **Portal STF**, Notícias STF, 07 maio 2020. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902>. Acesso em: 23 jul. 2020.

BRKAN, M. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. **International Journal of Law and Information Technology**, 11 jan. 2019. Disponível em:

[https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3124901](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901). Acesso em: 20 out. 2019.

CAMBRIDGE Analytica se declara culpada em caso de uso de dados no Facebook. **G1**, 09 jan. 2019. Disponível em:

<https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml>. Acesso em: 23 nov. 2019. Economia, Tecnologia.

CANO, R. J. Mais de 400 mil brasileiros foram afetados pelo vazamento de dados do Facebook. **El País**, Guadalajara, 05 abr. 2018. Tecnologia. Disponível em:

[https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235\\_618558.html](https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235_618558.html). Acesso em: 23 nov. 2019.

CASTELLS, M. **A sociedade em rede**: Vol. 1. 8.<sup>a</sup> ed. São Paulo: Paz e Terra, 2005.

CITRON, D. K.; PASQUALE, F. The scored society: due process for automated predictions. **Washington Law Review**, vol. 89, 2014, p. 1-33. Disponível em:

<https://ssrn.com/abstract=2376209>. Acesso em: 15 out. 2019.

COLAÇO, H. S. **Exercício do direito à autodeterminação informativa nas redes sociais**. 2017. Dissertação (Mestrado em Direito Constitucional) – Fundação Edson Queiroz, Universidade de Fortaleza, Fortaleza, 2017.

COLOMBO, C.; FACCHINI NETO, E. Mineração de dados e análise preditiva: reflexões sobre possíveis violações ao direito de privacidade na sociedade da informação e critérios para sua adequada implementação à luz do ordenamento brasileiro. **Revista de Direito**,

**Governança e Novas Tecnologias**, Maranhão, v. 3, n. 2, p. 59-80, jul./dez. 2017. Disponível em: [http://repositorio.pucrs.br/dspace/bitstream/10923/11454/2/Mineracao\\_de\\_dados\\_e\\_analise\\_preditiva\\_reflexoes\\_sobre\\_possiveis\\_violacoes\\_ao\\_direito\\_de\\_privacidade\\_na\\_sociedade\\_da.pdf](http://repositorio.pucrs.br/dspace/bitstream/10923/11454/2/Mineracao_de_dados_e_analise_preditiva_reflexoes_sobre_possiveis_violacoes_ao_direito_de_privacidade_na_sociedade_da.pdf) . Acesso em: 03 nov. 2019.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, D. *et al.* Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. Disponível em: <https://periodicos.unifor.br/rpen/article/view/8257/pdf>. Acesso em: 02 nov. 2019.

DONEDA, D. O direito fundamental à proteção de dados pessoais. *In*: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.<sup>a</sup> ed. Indaiatuba: Editora Foco, 2019, p. 35-53.

DONEDA, D.; CUNHA, M. V. A. Risco e Informação Pessoal: o Princípio da Finalidade e a Proteção de Dados no Ordenamento Brasileiro. **Revista Brasileira de Risco e Seguro**, Rio de Janeiro, v. 5, n. 10, p. 85-102, out. 2009/mar. 2010. Disponível em: <http://www.rbrs.com.br/arquivos/RBRs10-4%20Danilo%20Doneda.pdf>. Acesso em: 05 jun. 2019.

EDWARDS, L.; VEALE, M. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions?”. **IEEE Security & Privacy**, maio/jun. 2018, p. 46-54. Disponível em: <https://arxiv.org/pdf/1803.07540.pdf>. Acesso em: 20 out. 2019.

FERREIRA, D. R. Responsabilidade civil dos agentes de tratamento de dados: subjetiva ou objetiva? **Jota**, 20 nov. 2019. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/responsabilidade-civil-dos-agentes-de-tratamento-de-dados-subjetiva-ou-objetiva-20112019>. Acesso em: 28 nov. 2019. Opinião & Análise, Dados pessoais.

FRAZÃO, A. Algoritmos e inteligência artificial: Repercussões de sua utilização sobre a responsabilidade civil e punitiva das empresas. **Jota**, 15 maio 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/algoritmos-e-inteligencia-artificial-15052018>. Acesso em: 05 jun. 2019.

FRAZÃO, A. Data-driven economy e seus impactos sobre os direitos da personalidade: Indo além da privacidade e do controle dos dados pessoais. **Jota**, 17 jul. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade-17072018>. Acesso em: 02 jun. 2019. Tecnologia.

FRAZÃO, A. Fundamentos da proteção dos dados pessoais. Noções introdutórias para a compreensão da importância da Lei geral de Proteção de Dados. *In*: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 23-52.

FRAZÃO, A. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Jota**, 05 dez. 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/o-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-totalmente-automatizadas-05122018>. Acesso em: 02 jun. 2019. Tecnologia.

FRAZÃO, A. Objetivos e alcance da Lei geral de Proteção de Dados. *In*: FRAZÃO, A.; TEPEDINO, G.; OLIVA, M. D. (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: RT, 2019, p. 99-129.

GOMES, H. S. Lei da União Europeia que protege dados pessoais entra em vigor e atinge todo o mundo; entenda. **G1**, 25 maio 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/lei-da-uniao-europeia-que-protege-dados-pessoais-entra-em-vigor-e-atinge-todo-o-mundo-entenda.ghtml>. Acesso em: 23 nov. 2019. Economia, Tecnologia.

HARARI, Y. N. **Homo Deus: A Brief History of Tomorrow**. London: Vintage, 2017.

KAMARINOU, D.; MILLARD, C.; SINGH, J. Machine Learning with Personal Data. **Legal Studies Research Paper 247/2016**. Queen Mary University of London, 2016. Disponível em: <https://ssrn.com/abstract=2865811>. Acesso em: 25 out. 2019.

KOSMANN, E. L.; ENGELMANN, W. A teoria do fato jurídico e os direitos da personalidade: uma (re)leitura mediada pela Constituição. **Civilistica.com**. Rio de Janeiro, a. 7, n. 3, 2018, p. 8. Disponível em: <http://civilistica.com/a-teoria-do-fato-juridico/>. Acesso em: 04 nov. 2019.

LEONARDI, M. **Tutela e privacidade na Internet**. São Paulo: Saraiva, 2012.

MACHADO, F. I. S. **Privacidade e proteção de dados pessoais na sociedade da informação: profiling e risco de discriminação**. 2018. Dissertação (Mestrado em Direito) – Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2018.

MARRAFON, M. A.; MEDON, F. Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados. **Conjur**, 9 set. 2019. Disponível em:

<https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd>. Acesso em: 20 out. 2019. Constituição e Poder.

MARTINS, G. M. O direito ao esquecimento na internet. *In*: MARTINS, G. M.; LONGHI, J. V. R. (Coord.). **Direito digital: Direito privado e internet**. 2.<sup>a</sup> ed. Indaiatuba: Editora Foco, 2019, p. 67-93.

MENDES, G. F.; BRANCO, P. G. G. **Curso de Direito Constitucional**. 13<sup>a</sup> ed. rev. e atual. São Paulo: Saraiva Educação, 2018.

MORAES, M. C. B.. A constitucionalização do direito civil e seus efeitos sobre a responsabilidade civil. **Direito, Estado e Sociedade**, Rio de Janeiro, v. 9, n. 29, p. 233-258, jul/dez. 2006.

MORAES, M. C. B.. Ampliando os direitos da personalidade. **ResearchGate**, 2010. Disponível em: [https://www.researchgate.net/publication/288490662\\_Ampliando\\_os\\_direitos\\_da\\_personalidade](https://www.researchgate.net/publication/288490662_Ampliando_os_direitos_da_personalidade). Acesso em: 02 nov. 2019.

MORAES, M. C. B. Apresentação. *In*: RODOTÁ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 1-12.

MONTEIRO, R. L. Artigo Estratégico 39: Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. Rio de Janeiro, dez. 2018. Disponível em: <https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf>. Acesso em: 05 jun. 2019.

MULHOLLAND, C. A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?. **Migalhas**, 30 jun. 2020. Disponível em: <https://m.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-de-dados-pessoais-culpa-ou-risco>. Acesso em: 22 jul. 2020.

NOTO LA DIEGA, G. Against Algorithmic Decision-Making. **Northumbria Legal Studies Working Paper n. 2018/01**. University of Northumbria at Newcastle, 2018. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3135357](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135357). Acesso em: 20 out. 2019.

OPHER, A. *et al.* **The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization** [...]. IBM Global Services, New York, 2016. Disponível em: <https://www.ibm.com/downloads/cas/4JROLDQ7>. Acesso em: 28 out. 2019.

PARLAMENTO EUROPEU E DO CONSELHO. **Diretiva 95/46/CE**, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <https://eur-lex.europa.eu/eli/dir/1995/46/oj?locale=pt>. Acesso em: 9 jun. 2019.

PARLAMENTO EUROPEU E DO CONSELHO. **Regulamento 2016/679**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#d1e6949-1-1>. Acesso em: 23 nov. 2019.

PILATI; J. I.; OLIVO, M. V. C. Direito à privacidade: uma nova perspectiva. **Revista Novos Estudos Jurídicos** (Eletrônica), Itajaí, vol. 19, n. 1, p. 77-94, jan./abr. 2014. Disponível em: <https://siaiap32.univali.br/seer/index.php/nej/article/view/5543/2948>. Acesso em: 25 out. 2019.

PIRES, P. F. *et al.* Plataformas para a internet das coisas. *In*: MARTINELLO, M.; ROBEIRO, M. R. N.; ROCHA, A. A. R. (Org.) **Minicursos do XXXIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. Porto Alegre: Sociedade Brasileira de Computação, 2015, p. 110-169. Disponível em: <http://sbrc2015.ufes.br/wp-content/uploads/livro-texto-Minicursos.pdf>. Acesso em: 29 out. 2019

PRIVACIDADE. *In*: **MICHAELIS Dicionário Brasileiro da Língua Portuguesa**. São Paulo: Editora Melhoramentos, 2015. Disponível em: <http://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=privacidade>. Acesso em: 29 out. 2019.

PRIVACY. *In*: **CAMBRIDGE Dictionary**. Cambridge: Cambridge University Press, 2019. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles-portugues/privacy>. Acesso em: 29 out. 2019.

PRIVACY. *In*: **OXFORD Learner's Dictionaries**. Oxford: Oxford University Press, 2019, tradução nossa. Disponível em: <https://www.oxfordlearnersdictionaries.com/us/definition/english/privacy?q=privacy>. Acesso em: 29 out. 2019.

PRIVATUS. *In*: LEWIS, Charlton T. **An Elementary Latin Dictionary**. Nova Iorque: American Book Company, 1890, p. 650, tradução nossa. Disponível em: <https://archive.org/details/anelementarylat01lewigoog/page/n660>. Acesso em: 29 out. 2019.

REGULATING the internet giants. The world's most valuable resource is no longer oil, but data. **The Economist**, London, 06 maio 2017. Leaders. Disponível em: <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>. Acesso em: 27 out. 2019.

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

ROSENBERG, M; CONFESSORE, N.; CADWALLADR, C. How Trump Consultants Exploited the Facebook Data of Millions. **The New York Times**, 17 mar. 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 23 nov. 2019. Politics.

SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D. **Curso de Direito Constitucional**. 8.<sup>a</sup> ed. São Paulo: Saraiva Educação, 2019.

SARMENTO, D.; SOUZA NETO, C. P. **Direito Constitucional: Teoria, história e métodos de trabalho**. Belo Horizonte: Editora Fórum, 2012.

SELBST, A. D.; POWLES, J. Meaningful information and the right to explanation. **International Data Privacy Law**, vol. 7, n. 4, 2017, p. 233-242. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3039125](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125). Acesso em: 15 out. 2019.

SETZER, V. W. Dado, Informação, Conhecimento e Competência. **DataGramZero**, v. 0, n. 0, dez. 1999, p. 1-3. Disponível em: [www.brapci.inf.br/index.php/article/download/14562](http://www.brapci.inf.br/index.php/article/download/14562). Acesso em: 27 out. 2019.

SILVA, J. A. **Curso de Direito Constitucional Positivo**. 37.<sup>a</sup> ed. rev. e atual. São Paulo: Malheiros Editores, 2014.

SOLOVE, D. J. **The digital person: technology and privacy in the information age**. New York: New York University Press, 2004.

SOUZA, E. N.; SILVA, R. G. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direito e a enunciação de remédios. **Pensar**, Fortaleza, v. 24, n. 3, p.1-22, jul./set. 2019, p. 8. Disponível em: <https://periodicos.unifor.br/rpen/article/view/9407>. Acesso em: 02 nov. 2019.

SOUZA, L. R. M. Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro n. 5.276/2016. **Caderno**

**Virtual, IDP, Brasília** – DF, v.1, n. 41, 2018. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/cadernovirtual/article/view/3153/1484>. Acesso em: 23 nov. 2019.

TEFFÉ, C. S. Marco Civil da Internet: considerações sobre a proteção da liberdade de expressão, neutralidade da rede e privacidade. *In*: BECKER, D.; FERRARI, I.; (Coord.). **Regulação 4.0: Novas tecnologias sob a perspectiva regulatória**. São Paulo: RT, 2019, p. 133-159.

TEPEDINO, G. A tutela da personalidade no ordenamento civil-constitucional brasileiro. **Academia**, [2008?]. Disponível em: [https://www.academia.edu/31740015/A\\_tutela\\_da\\_personalidade\\_no\\_ordenamento\\_civil-constitucional\\_brasileiro](https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro). Acesso em: 20 jul. 2020.

TEPEDINO, G.. Premissas metodológicas para a constitucionalização do direito civil. **Revista de Direito do Estado**, Rio de Janeiro, ano 1, n. 2, p. 37-53, 2008.

VALENTE, J. Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy By Design e Privacy Enhancing Technologies. *In*: BRANCO, S.; TEFFÉ, C. (Org.). **Privacidade em Perspectivas**. Rio de Janeiro: Lumen Juris, 2018, p. 111-128.

VEDDER, A; NAUDTS, L. Accountability for the use of algorithms in a big data environment. **International Review of Law, Computers & Technology**, v. 31, Issue 2, p. 206-224, 08 mar. 2017, p. 5.

WACHTER, S.; MITTELSTADT, B.; FLORIDI, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, 2017. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em: 20 out. 2019.

<sup>1</sup>WHAT are bits, bytes, and other units of measure for digital information? **Indiana University**, Bloomington, 18 jan. 2018, tradução nossa. Disponível em: <https://kb.iu.edu/d/ackw>. Acesso em: 26 out. 2019.

ZANATTA, R. A. F. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. **ResearchGate**, fev. 2019. Disponível em: [https://www.researchgate.net/publication/331287708\\_Perfilizacao\\_Discriminacao\\_e\\_Direitos\\_do\\_Codigo\\_de\\_Defesa\\_do\\_Consumidor\\_a\\_Lei\\_Geral\\_de\\_Protecao\\_de\\_Dados\\_Pessoais](https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais). Acesso em: 03 nov. 2019.