

**UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI**  
**VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO**  
**PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM CIÊNCIA JURÍDICA – PPCJ**  
**CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ**  
**ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO**

**A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS  
PESSOAIS: REFLEXOS DO REGULAMENTO GERAL DE  
PROTEÇÃO DE DADOS EUROPEU (RGPD) NO ÂMBITO DA  
GARANTIA DE DIREITOS FUNDAMENTAIS NO DIREITO  
BRASILEIRO**

**VITOR SARDAGNA POETA**

**Itajaí-SC, abril de 2020**

**UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI**  
**VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E INOVAÇÃO**  
**PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU* EM CIÊNCIA JURÍDICA – PPCJ**  
**CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ**  
**ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO**

# **A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS PESSOAIS: REFLEXOS DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU (RGPD) NO ÂMBITO DA GARANTIA DE DIREITOS FUNDAMENTAIS NO DIREITO BRASILEIRO**

**VITOR SARDAGNA POETA**

Dissertação submetida ao Curso de Mestrado em Ciência Jurídica da Universidade do Vale do Itajaí – UNIVALI, como requisito parcial à obtenção do título de Mestre em Ciência Jurídica.

**Orientador: Professor Doutor Alexandre Moraes da Rosa**

**Itajaí-SC, abril de 2020**

## **AGRADECIMENTOS**

A Deus, causa primária de todas as coisas, pela dádiva da vida e pela oportunidade de acordar, todos os dias, e poder experimentar e degustar a existência terrestre.

Ao Prof. Dr. Alexandre Morais da Rosa, meu orientador, pelos conselhos, papos e conversas, mesmo que rápidas, diante de toda a “loucura” que é nosso dia a dia. Gratidão por ser mestre e amigo.

Aos colegas e amigos dessa jornada de mestrado, em especial, Christian Martins e Thiago Luiz Gesser Cesca. Vocês tornaram essa experiência muito mais suave, alegre e divertida.

À Univali, instituição em que este trabalho foi desenvolvido, por ter disponibilizado toda sua bela infraestrutura, bibliotecas, laboratórios e equipe (que é sensacional).

Aos meus guias, mentores e heróis (do presente e do passado). Obrigado por tanto.

Por fim, a todos aqueles que contribuíram, direta ou indiretamente, para a realização desta dissertação, o meu sincero agradecimento.

## **DEDICATÓRIA**

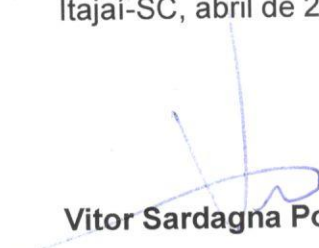
Aos meus pais, Renato Sardagna Poeta e Marilda Duarte Poeta, por sempre acreditarem em mim e por terem abdicado de suas vidas em prol das realizações e da felicidade de seus filhos.

À minha avó Edit, amor imensurável, que desde os meus primeiros passos fora meu grande alicerce, melhor amiga, incentivadora e maior fã.

## **TERMO DE ISENÇÃO DE RESPONSABILIDADE**

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, abril de 2020



**Vitor Sardagna Poeta**

**Mestrando**

## P Á G I N A   D E   A P R O V A Ç ã O

### MESTRADO

Conforme Ata da Banca de Defesa de Mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica PPCJ/UNIVALI, em 08/06/2021, às 10 horas, o mestrando VITOR SARDAGNA POETA fez a apresentação e defesa da Dissertação, sob o título “A INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS PESSOAIS: REFLEXOS DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS EUROPEU (RGPD) NO ÂMBITO DA GARANTIA DE DIREITOS FUNDAMENTAIS NO DIREITO BRASILEIRO”.

A Banca Examinadora foi composta pelos seguintes professores: Doutor Alexandre Moraes da Rosa (UNIVALI) como presidente e orientador, Doutora Keity Mara Ferreira de Souza e Saboya (UFRN) como membro, Doutor Alexandre José Mendes (PÓS-DOCTORADO UNIVALI) como membro e Doutora Maria Cláudia da Silva Antunes de Souza (UNIVALI) como membro suplente. Conforme consta em Ata, após a avaliação dos membros da Banca, a Dissertação foi Aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), dia 08 de junho de 2021.



PROF. DR. PAULO MÁRCIO DA CRUZ  
Coordenador/PPCJ/UNIVALI

## ROL DE ABREVIATURAS E SIGLAS

|                  |                                                                                       |
|------------------|---------------------------------------------------------------------------------------|
| AIPD             | Avaliação de Impacto na Proteção de Dados                                             |
| ANPD             | Autoridade Nacional de Proteção de Dados                                              |
| CGI.br           | Comitê Gestor da Internet no Brasil                                                   |
| CE               | Conselho Europeu                                                                      |
| CP               | Código Penal                                                                          |
| CPF              | Cadastro de Pessoas Físicas                                                           |
| CRFB             | Constituição da República Federativa do Brasil                                        |
| EAD              | Educação a Distância                                                                  |
| <i>E-Digital</i> | Estratégia Brasileira para a Transformação Digital                                    |
| EDPS             | <i>European Data Protection Supervisor</i>                                            |
| EUA              | Estados Unidos                                                                        |
| GDPR             | <i>General Data Protection Regulation</i>                                             |
| HIV              | Vírus da Imunodeficiência Humana                                                      |
| IA               | Inteligência Artificial                                                               |
| IBM              | <i>International Business Machines Corporation</i>                                    |
| ICMS             | Imposto sobre Operações relativas à Circulação de Mercadorias e Prestação de Serviços |
| IDC              | <i>International Data Corporation</i>                                                 |
| IEEE             | Instituto de Engenharia Elétrica e eletrônica                                         |
| IETF             | Força-Tarefa de Engenharia de Internet                                                |
| IHS              | Sistema Integrado de Informação em Saúde                                              |
| IOT              | Internet of Things (internet das coisas)                                              |
| IP               | <i>Internet Protocol</i>                                                              |
| LGPD             | Lei Geral de Proteção de Dados                                                        |
| MCI              | Marco Civil da Internet                                                               |
| MGD              | <i>Machine-generated data</i>                                                         |
| MIT              | Instituto de Tecnologia de Massachusetts                                              |
| NSA              | Agência Nacional de Segurança                                                         |
| OCDE             | Organização para a Cooperação e Desenvolvimento Econômico                             |
| ONG              | Organização Não-Governamental                                                         |

|       |                                                        |
|-------|--------------------------------------------------------|
| OPD   | Oficial de Proteção de dados                           |
| PIN   | Número de Identificação Pessoal                        |
| PLC   | Projeto de Lei Complementar                            |
| PPCJ  | Programa de Pós-Graduação em Ciência Jurídica          |
| PSDB  | Partido da Social Democracia Brasileira                |
| RG    | Registro Geral                                         |
| RGPD  | Regulamento Geral da Proteção de Dados                 |
| RIPD  | Rede Ibero-americana de Proteção de Dados              |
| STF   | Supremo Tribunal Federal                               |
| TICs  | Tecnologias da Informação e Comunicação                |
| UE    | União Europeia                                         |
| WiMAX | <i>Worldwide Interoperability for Microwave Access</i> |



## ROL DE CATEGORIAS

**Dados pessoais** - São informações que se referem a uma pessoa viva, identificada ou passível de identificação. Também são considerados como dados pessoais um agrupamento de informações diversas que podem levar uma determinada pessoa a ser identificada.

**Devassa de dados** – É a divulgação de dados de um determinado indivíduo sem a sua autorização.

**Direito à privacidade** - Conjunto de informações sobre um indivíduo que ele pode optar por manter sob seu controle, ou comunicar, decidindo a sobre quem, quando, onde e mediante quais condições, sem que possa ser legalmente sujeito a isso<sup>1</sup>.

**Inteligência Artificial** – Corresponde à habilidade de um programa de computador de desenvolver funções e raciocínio típicos da mente humana<sup>2</sup>.

**Proteção de Dados** – Garantia derivada da privacidade em que ocorre a tutela da personalidade do indivíduo, contra os potenciais riscos advindos do tratamento de dados pessoais. A sua função é a de proteger a pessoa titular dos dados e não os dados per si<sup>3</sup>.

---

<sup>1</sup> SILVA, José. Afonso da. **Curso de direito constitucional positivo**. 41 ed. São Paulo: Malheiros, 2018, p.208.

<sup>2</sup> BITTENCOURT, G. **Inteligência artificial**: ferramentas e teorias. 2. ed. Florianópolis: Editora da UFSC, 2001, p.16.

<sup>3</sup> MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. Série IDP: Linha Pesquisa Acadêmica. São Paulo: Saraiva, 2014. p. 32.

## SUMÁRIO

|                                                                                                    |      |
|----------------------------------------------------------------------------------------------------|------|
| <b>RESUMO</b>                                                                                      | p.12 |
| <b>ABSTRACT</b>                                                                                    | p.13 |
| <b>INTRODUÇÃO</b>                                                                                  | p.14 |
| <b>1 CONCEITOS E MOMENTOS HISTÓRICOS RELEVANTES NA PROTEÇÃO DE DADOS PESSOAIS E NA PRIVACIDADE</b> | p.17 |
| 1.1 DIREITOS E GARANTIAS FUNDAMENTAIS                                                              | p.17 |
| 1.2 A EVOLUÇÃO DA PROTEÇÃO DE DADOS E DA PRIVACIDADE NA LEGISLAÇÃO EUROPEIA                        | p.29 |
| 1.3 A EVOLUÇÃO DA PROTEÇÃO DE DADOS E DA PRIVACIDADE NA LEGISLAÇÃO BRASILEIRA                      | p.32 |
| 1.4 A INFLUÊNCIA DA TECNOLOGIA E A PRIVACIDADE NA SOCIEDADE ATUAL                                  | p.40 |
| <b>2 NOVAS TECNOLOGIAS E DITAMES ATUAIS</b>                                                        | p.49 |
| 2.1 A INTELIGÊNCIA ARTIFICIAL NOS DIAS ATUAIS                                                      | p.49 |
| 2.2 O USO DE BIG DATAS                                                                             | p.55 |
| 2.3 O LADO POSITIVO DAS NOVAS TECNOLOGIAS                                                          | p.56 |
| 2.4 O LADO NEGATIVO DAS NOVAS TECNOLOGIAS                                                          | p.59 |
| 2.5 SERVIÇOS TECNOLÓGICOS QUE INTEGRAM O TRATAMENTO DE DADOS                                       | p.65 |
| <b>3 PROTEÇÃO DE DADOS VERSUS TECNOLOGIA DA INFORMAÇÃO</b>                                         | p.73 |
| 3.1 DIREITOS CENTRAIS RELACIONADOS À PROTEÇÃO DE DADOS E À PRIVACIDADE                             | p.73 |
| 3.1.1 Direito à intimidade e à privacidade                                                         | p.73 |
| 3.1.2 Direito à autodeterminação informativa                                                       | p.77 |
| 3.2 OS DADOS PESSOAIS E SEUS TITULARES                                                             | p.80 |
| 3.3 O CONFRONTO: INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS                                     | p.88 |

**CONSIDERAÇÕES FINAIS**.....p.105

**REFERÊNCIAS DAS FONTES CITADAS**.....p.110

## RESUMO

A presente Dissertação está inserida na Linha de Pesquisa Constitucionalismo e Produção do Direito e objetiva verificar, com base na doutrina, legislação e jurisprudência se a proteção trazida pela Lei Geral de Proteção de dados tem sido suficiente para resguardar o direito fundamental à privacidade em tempos de massificação dos dados e evolução tecnológica. Para tanto, apresenta os conceitos e momentos históricos relevantes na proteção dos dados pessoais e da privacidade; trata das novas tecnologias frente aos ditames atuais, dando-se ênfase ao atual uso da inteligência artificial nos tempos modernos; e contrapõe a proteção de dados ao desenvolvimento tecnológico. Como metodologia foi empregada a pesquisa teórico-dogmática, tendo em vista que foi realizada uma revisão de literatura em doutrinas, legislações e jurisprudências com vistas a encontrar uma solução para mitigar o conflito que se formou em torno do direito à privacidade e o direito à informação. Ao final do estudo concluiu-se que não obstante o tratamento jurídico dispensado aos dados pessoais dos cidadãos no Brasil não tenha sido suficiente para resguardar o direito fundamental à privacidade em tempos de massificação dos dados, o Brasil tem caminhado no sentido de assegurar que o direito à privacidade seja resguardado, sem, no entanto, obstar o desenvolvimento da tecnologia da informação.

**Palavras-chave:** Lei Geral de Proteção de Dados. *Big Data*. Inteligência artificial. Privacidade. Intimidade.

## **ABSTRACT**

This dissertation is part of the line of research Constitutionalism and Production of Law. It aims to verify, based on doctrine, legislation and jurisprudence, whether the protection provided by the General Data Protection Law has been sufficient to safeguard the fundamental right to privacy in times of massification of data and technological evolution. It presents the concepts and historical milestones in the protection of personal data and privacy; addresses the new technologies used to deal with the current demands, in particular, the use of artificial intelligence; and examines the conflict between data protection to technological development. The theoretical-dogmatic research method is used, with a review of the literature on doctrine, laws and jurisprudence, seeking to find a solution that can mitigate the conflict between the right to privacy and the right to information. At the end of the study, it is concluded that despite the legal treatment given to the personal data of citizens in Brazil, this has not been sufficient to safeguard the fundamental right to privacy in times of massification of data. However, Brazil is moving towards ensuring that the right to privacy is safeguarded, without hindering the development of information technology.

**Keywords:** General Data Protection Law. Big data. Artificial intelligence. Privacy. Confidentiality

## INTRODUÇÃO

Vive-se hoje uma época de grande “exposição midiática”. As pessoas não conseguem mais viver desconectadas e diariamente um volume muito grande de informação e dados pessoais são despejados na internet viabilizando uma diversidade de violações aos direitos fundamentais. Essas violações, a seu turno, têm levado ao surgimento de esforços para contê-las, a exemplo da Lei Geral de Proteção de Dados (LGPD), levando a pensar sobre até que ponto seria razoável restringir a divulgação destas informações na Web ante ao risco de gerar um colapso no avanço tecnológico.

O objetivo institucional da presente Dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali.

O seu objetivo científico é analisar como o RGPD/2016/679 e a Lei n. 13.709, de 14 de agosto de 2018, podem influenciar, positiva ou negativamente, em novos ditames tecnológicos, principalmente no quesito “Inteligência Artificial”, analisando-se, primordialmente o regulamento e a lei citados acima, verificando como os institutos legais podem salvaguardar a proteção de dados pessoais, com o advento das novas tecnologias, reflexionando se as atuais legislações protegem, de fato, os dados de pessoas naturais.

Para a pesquisa foram levantadas as seguintes hipóteses:

a) O RGPD/2016/679 e a Lei n. 13.709, de 14 de agosto de 2018, são capazes de salvaguardar os direitos inerentes à proteção de dados e privacidade do ser humano.

b) O mal tratamento de dados da pessoa singular acarreta em ofensas diretas aos direitos fundamentais relativos à dignidade, liberdade, privacidade, intimidade, honra e à imagem.

c) O posicionamento jurisprudencial dominante, com o advento da Lei n.13.709/2018 tem se esforçado em assegurar que o direito à privacidade seja

resguardado, sem, no entanto obstar o desenvolvimento da tecnologia da informação.

Os resultados do trabalho de exame das hipóteses estão expostos na presente dissertação, de forma sintetizada, como segue.

Principia-se, no Capítulo 1, apresentando os conceitos e momentos históricos relevantes na proteção de dados pessoais e privacidade. Para tanto, discute os direitos e garantias fundamentais, a evolução da proteção de dados e privacidade na legislação europeia, a evolução da proteção de dados e privacidade na legislação brasileira bem como a influência da tecnologia sobre a privacidade na sociedade atual.

O Capítulo 2 trata das novas tecnologias frente aos ditames atuais. Assim, explica o atual uso da inteligência artificial nos tempos modernos; o uso de *Big Dates*; o lado positivo e o negativo das novas tecnologias; e, os serviços tecnológicos que integram o tratamento de dados.

Por fim, o Capítulo 3 dedica-se a contrapor a proteção de dados ao desenvolvimento tecnológico. Neste contexto, explica os direitos centrais relacionados à proteção de dados e à privacidade; expõe o tratamento dado aos dados pessoais; e no confronto entre inteligência artificial e proteção de dados, busca encontrar caminhos para conciliar estas duas realidades tendo em vista que não se mostra razoável limitar excessivamente a divulgação de dados pessoais e nem permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação.

O presente Relatório de Pesquisa se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões sobre a inteligência artificial e a proteção de dados pessoais com vistas a expandir os conhecimentos sobre os reflexos do RGPD no âmbito da garantia de direitos fundamentais no Direito brasileiro.

O Método utilizado na fase de Investigação<sup>4</sup> foi o Método Indutivo<sup>5</sup>; na fase de Tratamento dos Dados foi o Método Cartesiano<sup>6</sup>, e, o Relatório dos Resultados expresso na presente Dissertação é composto na base lógica indutiva.

Nas diversas fases da Pesquisa, foram acionadas as Técnicas do Referente<sup>7</sup>, da Categoria<sup>8</sup>, do Conceito Operacional<sup>9</sup> e da Pesquisa Bibliográfica<sup>10</sup>.

As Técnicas de investigação foram definidas pelo mestrando e por seu orientador, levados em consideração os parâmetros adotados pelo Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica – PPCJ/UNIVALI, e mencionadas aqui, com a indicação das fontes que foram efetivamente utilizadas para compor a Dissertação.<sup>11</sup>

Nesta Dissertação as Categorias principais<sup>12</sup> estão grafadas com a letra inicial em maiúscula e os seus Conceitos Operacionais são apresentados em glossário inicial.<sup>13</sup>

---

<sup>4</sup> “[...] momento no qual o Pesquisador busca e recolhe os dados, sob a moldura do Referente estabelecido [...]” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. 13 ed. Florianópolis: Conceito Editorial, 2015. p. 87).

<sup>5</sup> “[...] pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral [...]” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. Op. cit., p. 91).

<sup>6</sup> Sobre as quatro regras do Método Cartesiano (evidência, dividir, ordenar e avaliar) veja LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001. p. 22-26.

<sup>7</sup> “[...] explicitação prévia do(s) motivo(s), do(s) objetivo(s) e do produto desejado, delimitando o alcance temático e de abordagem para a atividade intelectual, especialmente para uma pesquisa” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática, p. 58).

<sup>8</sup> “[...] palavra ou expressão estratégica à elaboração e/ou à expressão de uma ideia” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. Op. cit., p. 27).

<sup>9</sup> “[...] uma definição para uma palavra ou expressão, com o desejo de que tal definição seja aceita para os efeitos das ideias que expomos [...]” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. Op. cit., p. 39).

<sup>10</sup> “Técnica de investigação em livros, repertórios jurisprudenciais e coletâneas legais” (PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. Op. cit., p. 215).

<sup>11</sup> Sobre Métodos e Técnicas vide: PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica**: Teoria e Prática. Op. cit., p.89-115.

<sup>12</sup> Dados Pessoais, Devassa de Dados, Direito à Privacidade, Inteligência Artificial e Proteção de Dados.

<sup>13</sup> Sobre Categorias e Conceitos Operacionais vide: PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica**: Teoria e Prática. Op. cit., p.31-60.



## CAPÍTULO 1

### CONCEITOS E MOMENTOS HISTÓRICOS RELEVANTES NA PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

Neste Capítulo serão apresentados os conceitos e momentos históricos relevantes na proteção de dados pessoais e privacidade. Para tanto, discute-se os direitos e garantias fundamentais, a evolução da proteção de dados e privacidade na legislação europeia, a evolução da proteção de dados e privacidade na legislação brasileira bem como a influência da tecnologia sobre a privacidade na sociedade atual.

#### 1.1 DIREITOS E GARANTIAS FUNDAMENTAIS

Inicia-se esta seção trazendo uma abordagem histórica dos direitos fundamentais, tendo em vista que essa evolução mantém relação de proximidade com a caracterização desses direitos, revelando também aspectos da evolução da sociedade tal como esta encontra-se hoje. Segundo Paulo Márcio Cruz e Alice Francisco da Cruz Salles:

A análise histórica torna-se extremamente útil para se explicitar a evolução e classificar os direitos e garantias fundamentais segundo seu conteúdo, tendo em vista que, a partir do início do constitucionalismo, é possível distinguir diversas “dimensões” de direitos, segundo os problemas ou condições do momento histórico em que foram desenvolvidos<sup>14</sup>.

Os direitos fundamentais surgiram da necessidade de proteger o homem do poder estatal, a partir dos ideais advindos do Iluminismo, no século XVIII, mais particularmente com o surgimento das constituições escritas. É imperioso ressaltar, contudo, que os direitos e garantias fundamentais não se restringem àquela função de limitar a atuação estatal, de modo a proteger o indivíduo de possíveis

---

<sup>14</sup> CRUZ, Paulo Márcio; SALLES, Alice Francisco da Cruz. Considerações sobre os direitos fundamentais sociais prestacionais e a sua concretização pelo poder judiciário. **Revista Eletrônica Direito e Política**, Programa de Pós Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.6, n.3, 2011. Disponível em: [www.univali.br/direitoepolitica](http://www.univali.br/direitoepolitica). Acesso em: 8 abr. 2020.

arbitrariedades cometidas pelo poder público, hipótese em que são conhecidos como liberdades negativas<sup>15</sup>.

Com efeito, a verdade é que os direitos fundamentais também têm por função permitir que o indivíduo possa participar, de maneira efetiva, do processo político do Estado a que esteja vinculado, não só por meio do exercício do voto e dos demais mecanismos de participação popular, como também se candidatando a ser um representante do povo na condução daquele mesmo Estado. Tem-se aí os chamados direitos políticos, também conhecidos como liberdades-participação.

Por outro lado, sabe-se que os Estados têm ampliado consideravelmente o conteúdo de suas constituições, buscando trazer para o corpo delas alguns temas que, à época do liberalismo clássico, não figuravam naqueles diplomas normativos. Esse fenômeno coincidiu com o surgimento do denominado Estado social (*Welfare State*), iniciado com a Constituição Mexicana de 1917, porém notabilizado com a Constituição de Weimar (atual Alemanha) de 1919<sup>16</sup>.

Portanto, as cartas magnas dos muitos Estados internacionais passaram a prever, de maneira cada vez mais intensa, diversas hipóteses de intervenção estatal na vida privada. Ao invés de conter apenas regras de regência do Estado e de proteção dos indivíduos contra o poder estatal, passaram também a conter um conjunto de normas de ordem social, cultural e econômica, tanto para a redução das desigualdades sociais, como também para incentivar o desenvolvimento nacional e foi neste contexto que surgiram os direitos fundamentais.

O indivíduo se comporta socialmente baseado em crenças religiosas e ideológicas, em princípios morais e éticos e, muitas vezes, sob limitantes problemas biológicos e sociais. Os comportamentos humanos, os quais se exteriorizam de maneira positiva ou negativa, consciente ou inconscientemente, são a origem da necessidade das leis. Atos que trazem prejuízos ao meio ambiente podem gerar danos morais. Deste modo, enquanto não cessar os excessos cometidos é

---

<sup>15</sup> SANTOS, Gustavo Ferreira. **Neoconstitucionalismo, Poder Judiciário e Direitos Fundamentais**. Curitiba: Juruá Editora, 2011, p. 63.

<sup>16</sup> SANTOS, Gustavo Ferreira. **Neoconstitucionalismo, Poder Judiciário e Direitos Fundamentais**. Curitiba: Juruá Editora, 2011, p. 64.

imperativo ao Estado assumir a função de tutelar, garantir e promover a defesa dos direitos fundamentais explicitados na CRFB/1988. Nesse sentido se manifesta Marcelo Schenk Duque:

Os direitos fundamentais afirmam-se como elementos de ordenação das pessoas para a coletividade. Os bens e interesses jurídicos que em geral são objeto de tutela pelos direitos fundamentais não foram criados pelo Estado, haja vista que possuem uma origem considerada pré-Estatal. [...] Trata-se de bens do mais alto significado, que se originaram não da ação estatal em si, mas no mundo dos fatos e que na acepção do Estado de direito, devem ser protegidos pelo Estado<sup>17</sup>.

Os direitos fundamentais, quando entendidos em sua dimensão objetiva, consubstanciam-se no pressuposto de um dever do Estado de atuar de forma eficaz, protegendo os indivíduos da atuação de outros, o que, se não ocorrer, poderá ensejar, até mesmo a responsabilização dos poderes públicos na esfera civil devido à omissão.

Assim, neste trabalho parte-se da premissa de que Constituição e direitos fundamentais protagonizaram e continuam a protagonizar, conjuntamente, o processo de limitação do poder estatal, a implantação da noção de Estado de Direito; trata-se da estruturação jurídica do Estado por meio de um documento que abarca as escolhas básicas, assegurando o estatuto do indivíduo diante do poder estatal.

O Estado Constitucional, em primeiro lugar, é aquele cuja estruturação se encontra em uma Constituição e vem acompanhada, necessariamente, pela previsão e garantia de direitos fundamentais; Estado cujo poder se limita pela Constituição e encontra fundamento nos direitos fundamentais. Segundo Sarlet<sup>18</sup>, o papel da Constituição, nesse modelo estatal, é fundamental, já que é em tal documento que se firma o estatuto relacional dos indivíduos com o Estado e entre si, bem como se estrutura o próprio Estado. A Constituição é o topo da ordem jurídica do Estado Constitucional ao congregar em si as decisões mais importantes da

---

<sup>17</sup> DUQUE, Marcelo Schenk. **Curso de direitos fundamentais**: teoria e prática. São Paulo: Revista dos Tribunais, 2014, p.52.

<sup>18</sup> SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado, 2012, p.34.

comunidade política.

O que se deseja enfatizar é a natureza normativa, ou seja, entender a Constituição como verdadeira norma jurídica neste modelo; uma Constituição normativa é aquela que efetivamente domina o processo político ao garantir o seu desenrolar democrático e, além disso, regula, em certa medida, os direitos fundamentais, não apenas os enunciando. Além disso, como expõe Carvalho<sup>19</sup>, uma das características que melhor define o atual Estado Constitucional é a imposição ao Estado de proteger os direitos, mesmo que o realize à margem da lei ou inclusive em posição/condição que supere os parâmetros da legalidade, visto que não se trata da eficácia dos direitos fundamentais na medida e nos termos demarcados na lei, mas se consubstancia na eficácia dos direitos fundamentais na medida e nos termos estabelecidos na Constituição. Em alusão ao princípio da supremacia da Constituição implica que as normas constitucionais e, em especial, os direitos fundamentais nela consagrados situam-se no topo da hierarquia do sistema normativo, de modo que todos os outros atos normativos existentes, a exemplo dos atos do Executivo e do Judiciário, e também todo ato jurídico precisam adotar como critério de medida o texto constitucional e os direitos fundamentais.

Conforme enfatiza Sarlet “os direitos fundamentais [...] nascem e se desenvolvem com as Constituições nas quais foram reconhecidos e assegurados”<sup>20</sup>. Verifica-se que a ideia de direitos fundamentais está atrelada com a ideia de constitucionalismo, pois os direitos fundamentais surgiram com a necessidade de proteger o homem do abuso de poder advindo do Estado, a partir dos ideais provenientes do Iluminismo nos séculos XVII e XVIII.

A partir do segundo pós-guerra, as constituições em grande parte dos Estados mudaram sua estrutura, passando de constituições sintéticas, que regulavam apenas a divisão dos poderes e a segurança pública, para constituições analíticas, que incorporaram toda a lógica de valores e princípios construídos pela

---

<sup>19</sup> CARVALHO, Osvaldo Ferreira de. **Restrições aos Direitos Fundamentais no Estado Constitucional**. Curitiba: Juruá Editora, 2019, p.158.

<sup>20</sup> SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado, 2012, p.35.

humanidade ao longo da história. Estes direitos quando adentram ao ordenamento jurídico de um país recebem a denominação de direitos fundamentais. Para sua caracterização, os direitos fundamentais recebem da doutrina dois critérios formais, quais sejam: 1) são designados direitos fundamentais os direitos ou garantias elencados no instrumento constitucional; 2) são aqueles direitos que recebem da Constituição um maior grau de garantia ou segurança; ou são imutáveis ou pelo menos de mudança dificultada<sup>21</sup>.

Direitos, garantias e deveres é a tríade que regula a vida em sociedade de todo e qualquer cidadão, porém, para que estas três grandezas jurídicas tenham valor jurídico e sejam respeitadas, precisam estar definidas e asseguradas por meio de leis contidas na Constituição de um país. No Estado brasileiro estas grandezas foram dispostas e referendadas como dispositivos de lei obrigatórios na CRFB/1988. É evidente que enquanto ser social, os direitos básicos de todo ser humano devem ser respeitados, salvaguardados, garantidos e obedecidos pelo Estado. Sendo assim, os direitos humanos positivados em uma determinada ordem social recebem a denominação de direitos fundamentais.

Com a instituição da CRFB/1988, que possui como um de seus princípios fundamentais a dignidade da pessoa humana, os direitos fundamentais tornaram-se objetos primordiais à ordem constitucional, já que constituem os elementos jurídicos necessários para a proteção da existência humana com dignidade. Nas palavras de Brega Filho os direitos fundamentais “são os interesses jurídicos previstos na Constituição que o Estado deve respeitar e proporcionar às pessoas a fim de que elas tenham uma vida digna”<sup>22</sup>.

Colocar a salvo a integridade dos indivíduos em seus aspectos mais extensos constitui-se em uma das finalidades e razões para a criação das leis, as quais têm como principal escopo facilitar e beneficiar as relações cooperativas de vida em sociedade. Entretanto, a manutenção da ordem social plena só será possível quando cada cidadão respeitar suas responsabilidades individuais.

---

<sup>21</sup> BONAVIDES, Paulo. **Curso de Direito Constitucional**. 33. ed. São Paulo: Malheiros, 2018, p.563.

<sup>22</sup> BREGA FILHO, Vladimir. **Direitos fundamentais na Constituição de 1988**: conteúdo jurídico das expressões. São Paulo: Juarez de Oliveira, 2002, p.67.

Referente aos direitos fundamentais, Sarlet<sup>23</sup> coloca que uma das mais importantes inovações é a trazida pelo art. 5º, § 1º, da CRFB/1988, pois segundo este dispositivo consigna, as normas que definem direitos fundamentais têm aplicabilidade imediata, a princípio excluindo a natureza programática destes preceitos. Mesmo assim ficou assegurada a supremacia dos direitos fundamentais na CRFB/1988 e importa destacar, ainda, a proteção trazida pelo art. 60, § 4º, que é o artigo em que as cláusulas pétreas são estabelecidas.

Verifica-se assim que no ordenamento jurídico brasileiro, os Direitos Fundamentais estão precipuamente listados nos arts. 5º a 17º da CRFB/1988, sem esquecer, é claro, da chamada abertura material do catálogo, previsto nos §§ 2º e 3º do art. 5º da Constituição<sup>24</sup>.

Além de tais classificações, existem princípios que orientam a interpretação e aplicação dos direitos fundamentais, tais como: supremacia da Constituição; eficácia direta; eficácia vinculante e eficácia irradiante. Estes princípios informam e estruturam o sistema a partir de um âmbito objetivo (ordem de valores) e subjetivo (direitos passíveis de ser exigidos por todos os participantes da ordem jurídica). Sendo assim, toda a discussão jurídica é realizada dentro de um mesmo sistema, que deve ser construído com base na coesão legislativa, e toda a inconsistência ou lacuna precisa ser expurgada através de controle de constitucionalidade, o que é bastante comum no Brasil.

Isto porque, como bem pontua Lênio Streck<sup>25</sup>, mesmo em tempos de Constituição democrática, no que diz respeito aos direitos fundamentais, vivencia-se uma crise de efetividade, pois, quando os direitos dos excluídos sociais (e também

---

<sup>23</sup> SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado, 2012, p.36.

<sup>24</sup> “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. § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais”.

<sup>25</sup> STRECK, Lênio Luiz. *Hermenêutica, Estado e Política: uma visão do papel da Constituição em países periféricos*. In CADEMARTORI, Daniela Mesquita Leutchuk; GARCIA, Marcos Leite (org.). **Reflexões sobre Política e Direito**. Homenagem aos Professores Osvaldo Ferreira de Melo e Cesar Luiz Pasold. Florianópolis: Conceito Editorial, 2008, p.231-233.

digitais), a Constituição parece ser apenas uma carta de intenções.

Neste contexto de crise de efetividade, Cesar Luiz Pasold propõe que “o Estado Contemporâneo tenha e exerça uma função social [...] respeitando, valorizando e envolvendo o seu sujeito, [...] sempre com a prevalência do social e privilegiando os valores fundamentais do ser Humano”<sup>26</sup>.

Outro ponto relevante a respeito dos direitos fundamentais reside na necessidade de compreender que estes não são absolutos. Eles podem conflitar e, nestes, casos, um irá se sobrepor a outro(s), situação em que será necessário proceder à ponderação de princípios.

Segundo ensina Jane Reis Gonçalves Pereira<sup>27</sup>, a presença de comandos e proibições condicionantes do comportamento humano é peculiar à própria ideia de ordenamento jurídico. Com efeito, para além dos preceitos permissivos, o sistema jurídico é composto, fundamentalmente, de uma série de normas que de diversas maneiras circunscrevem a liberdade das pessoas.

As limitações aos direitos fundamentais materializam-se de várias formas. Segundo Carvalho<sup>28</sup>, há certas hipóteses em que a ausência de lastro jurídico que legitimem certas ações humanas não advém de intervenções legislativas nos direitos, mas do seu próprio perfil traçado na Constituição. Em outros casos, o legislador possui autorização constitucional para definir ou modular os contornos do Direito. E, quando o Judiciário faz uso do método da ponderação de interesses, tem-se que a limitação ao direito fundamental ocorre *in concreto* por meio do afastamento de sua incidência numa hipótese específica.

Carvalho<sup>29</sup> explica que as restrições de direitos fundamentais são normas que estabelecem privações ou supressões de certas formas de exercício dos direitos

---

<sup>26</sup> PASOLD, Cesar Luiz. **Função Social do Estado Contemporâneo**. 4 ed. Itajaí: Univali, 2013, p.52.

<sup>27</sup> PEREIRA, Jane Reis Gonçalves. **Interpretação constitucional e direitos fundamentais**: uma contribuição ao estudo das restrições aos direitos fundamentais na perspectiva da teoria dos princípios. Rio de Janeiro: Renovar, 2006, p.111.

<sup>28</sup> CARVALHO, Osvaldo Ferreira de. **Restrições aos Direitos Fundamentais no Estado Constitucional**. Curitiba: Juruá Editora, 2019, p.161.

<sup>29</sup> Ibidem, p.162.

que, partindo-se de uma interpretação ampliativa, estariam compreendidas no âmbito de proteção dos preceitos constitucionais que os consagram.

Ao afirmar que as restrições são normas, cumpre consignar que, como destaca Robert Alexy, “[...] uma norma pode ser uma restrição de direito fundamental só se é constitucional”<sup>30</sup>. Dessa forma, as restrições – para serem entendidas como tais – hão de mostrar-se constitucionalmente legítimas.

Lembra Duque<sup>31</sup> que a restrição poderá ser versada em lei geral ou ser produto da interpretação jurídica levada a efeito pelo Poder Judiciário, ou seja, ela pode surgir não apenas em abstrato, no ato legislativo, mas pode também aparecer no momento aplicativo.

A CRFB/1988<sup>32</sup>, em seus artigos 1º e 5º, estendeu o reconhecimento dos Direitos Fundamentais, mas paralelamente foram ampliadas as possibilidades de colisões entre Direitos, fruto não apenas da Constituição, mas das mudanças na sociedade e no papel do Judiciário, o que faz surgir a necessidade de uma técnica racional de análise e de resolução de controvérsias, de procedimentos que permitam decisões coerentes, capazes de inibir lesão a Direitos e a discricionariedade.

Assim, não cabe apenas recorrer à subsunção. Abre-se espaço à ponderação. Mas ela não pode ser irracional, já que os Direitos Fundamentais são constituídos de valores às vezes conflitantes e difíceis de serem harmonizados. Deve-se, portanto, buscar concretizar os Direitos de maneira fundamentada, observando requisitos que reduzam ou domesticuem a discricionariedade ínsita à ponderação.

Desta forma, surge o debate no âmbito nacional quanto às restrições a Direitos Fundamentais. No entanto, no Brasil essas restrições não estão expressas na Constituição, mas baseando-se em parâmetros de Direito comparado percebe-se

---

<sup>30</sup> ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público), p.244.

<sup>31</sup> DUQUE, Marcelo Schenk. **Curso de direitos fundamentais**: teoria e prática. São Paulo: Revista dos Tribunais, 2014, p.55.

<sup>32</sup> BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm). Acesso em: 21 Fev. 2020.



a necessidade de serem delimitados limites aos limites.

Daí surge a teoria externa e a interna que de forma diferente tentam encontrar o entendimento sobre limites ou restrições, conforme explana Afonso da Silva:

Enquanto as teorias externas [...] – não somente aceitam como também pressupõem – em quase todos os casos – a necessidade de restrição a Direitos fundamentais, os adeptos de teorias internas utilizam o conceito de limite para rejeitar essa necessidade. A contraposição entre definição de limites, de um lado, e imposição de restrições, de outro, explicita as diferenças entre os dois enfoques<sup>33</sup>.

A teoria externa, de caráter liberal, identifica os Direitos fundamentais como uma maneira de obstar a intervenção do poder estatal na esfera privada. A teoria externa entende por restrições determinações que são externas aos Direitos, ou seja, vêm de fora, que teriam de ser previstas expressamente na Constituição, e que deveria prevalecer a liberdade. A regra é a não intervenção. A restrição amputa, diminui o âmbito do Direito. Por isso deveria ser expressamente prevista, deveria ser veiculada por lei, respeitar a igualdade, ser proporcional.

Já a teoria interna surge com o entendimento de limites que são imanentes, ou seja, que são internos aos Direitos, que são barreiras a eles. De certa forma, a teoria interna entende que existiria uma reserva de intervenção colocada ao legislador o que de certa forma tem o sentido inverso ao da teoria externa, que limita as intervenções nos Direitos, ou seja, permite uma intervenção maior do Estado. Conforme Novais<sup>34</sup>, a teoria interna imanente revela uma fronteira ao conteúdo do Direito.

A teoria interna segundo Silva<sup>35</sup> traz o entendimento de limites imanentes, desta forma, os Direitos Fundamentais não seriam absolutos, tendo em vista, possuírem limites constitucionais, implícitos ou explícitos.

---

<sup>33</sup> SILVA, José. Afonso da. **Curso de direito constitucional positivo**. 41 ed. São Paulo: Malheiros, 2018, p.131.

<sup>34</sup> NOVAIS, Jorge Reis. **As Restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição**. Coimbra: Coimbra Editora, 2003, p.77.

<sup>35</sup> SILVA, José. Afonso da. **Curso de direito constitucional positivo**. 41 ed. São Paulo: Malheiros, 2018, p.132.

Novais<sup>36</sup> aduz que quando se fala de limites entende-se que serão declarados limites previamente existentes, já quando se trata de restrição seria algo constituído, como uma nova restrição, algo que não seria imanente, não estaria na Constituição. Então, quando se observam colisões entre Direitos fundamentais, consoante a teoria interna seriam declarados limites constitucionais e não restrições, destacadas do Direito, conforme expressa a teoria externa.

Uma das críticas à teoria externa identifica nela uma insegurança jurídica, pois existiria um Direito *prima facie* que geraria uma expectativa de sopesamento entre princípios para a solução dos confrontos entre os Direitos fundamentais.

Assim, na sociedade cada vez mais complexa e, em consequência, com problemas também mais complexos, aumenta a ocorrência de colisões entre Direitos fundamentais. Observa-se que ambas as teorias são extremadas. Segundo Vieira<sup>37</sup>, a primeira, liberal e garantista, limita a intervenção do Estado na promoção de interesses públicos que se chocam com liberdades individuais; a segunda é mais favorável à intervenção do Estado, mas deixa fluidos os limites de tal intervenção, ameaçando a liberdade.

Por isso, parece mais interessante um entendimento intermediário, que leve em consideração os valores envolvidos na situação específica por meio da ponderação que, conforme Barroso é uma “técnica de decisão jurídica, aplicável a casos difíceis, em relação aos quais a subsunção se mostrou insuficiente”<sup>38</sup>. Pode-se aproveitar também os limites aos limites (legalidade, igualdade, proporcionalidade, não-retroatividade) como critérios que podem auxiliar na resolução das controvérsias.

Destaca-se a necessidade de coerência e integridade na jurisprudência para assegurar que as colisões que eventualmente surjam, sejam adequadamente solucionadas e que não existam posições que não respeitem a Constituição, ou,

---

<sup>36</sup> NOVAIS, Jorge Reis. **As Restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição**. Op. cit., p.80.

<sup>37</sup> VIEIRA, Oscar Vilhena. **Direitos fundamentais**: uma leitura da jurisprudência do STF. São Paulo Malheiros, 2016, p.133.

<sup>38</sup> BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009, p.334.

sejam discricionárias ou subjetivas, devendo haver coerência e integridade em decisões que busquem resolver colisões entre tais Direitos. A exigência de coerência e de integridade decorre da teoria da argumentação jurídica, a partir de autores como Dworkin<sup>39</sup>, e pode auxiliar na resolução de referidas colisões fazendo uso da ponderação.

A ponderação de princípios é fundamental para que se solucione a questão da colisão de princípios. Outra denominação encontrada para essa atividade é a de sopesamento. Para Ávila “consiste num método destinado atribuir pesos a elementos que se entrelaçam”<sup>40</sup>.

Cabe ressaltar que em caso de colisão de princípios, um deles tem precedência em face do outro a depender de determinadas condições. Sob outras condições a precedência pode ser estabelecida de forma diversa<sup>41</sup>. Assim, não há uma determinação geral para todas as situações de colisão de princípios, o caso concreto é que vai estabelecer qual dos princípios em conflito terá precedência.

Diante disso, a proporcionalidade é o critério, como entendem alguns doutrinadores, ou o princípio norteador, como entendem outros, para solução desse conflito. A ideia da proporcionalidade, bastante aceita e difundida no pensamento jurídico-constitucional contemporâneo, teve sua origem, segundo Bonavides<sup>42</sup> na década de 1950 na doutrina alemã e desenvolvida pela jurisprudência do Tribunal Constitucional Federal alemão foi recepcionada pela doutrina e jurisprudência de vários países do mundo, inclusive o Brasil.

Partindo da premissa sugerida por Alexy<sup>43</sup> de que os princípios são mandamentos visando à otimização e se caracterizam por poderem ser observados em graus diversos, contanto que sejam realizados sempre que possível e atendendo às possibilidades fáticas e jurídicas existentes, o autor aduz que o princípio da

---

<sup>39</sup> DWORKIN, Ronald. **Levando os Direitos a sério**. São Paulo: Martins Fontes, 2002, p.69.

<sup>40</sup> ÁVILA, Humberto. **Teoria dos Princípios**. 18. ed. São Paulo: Malheiros, 2018, p.143.

<sup>41</sup> ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público), p.116.

<sup>42</sup> BONAVIDES, Paulo. **Curso de Direito Constitucional**. 33. ed. São Paulo: Malheiros, 2018, p.568.

<sup>43</sup> ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público), p.116.

proporcionalidade decorre logicamente da natureza dos princípios, por isso há uma conexão entre a teoria dos princípios e a máxima da proporcionalidade, incluídas aí suas máximas parciais da adequação, necessidade e proporcionalidade em sentido estrito. Referente à adequação, esta seria a relação entre meio e fim da escolhida feita. A necessidade seria a questão do meio menos restritivo ao direito fundamental escolhido, dentre os meios disponíveis. Essas duas decorrem da natureza dos princípios como mandamentos e otimização, em face das possibilidades fáticas. A proporcionalidade em sentido estrito se refere ao próprio sopesamento, que nos dizeres de Alexy “decorre da relativização em face das possibilidades jurídicas”<sup>44</sup>. Nas ponderações de Ávila esse sopesamento “exige a comparação entre a importância da realização do fim e a intensidade da restrição dos direitos fundamentais”<sup>45</sup>.

Retornando à teoria externa sobre a restrição dos direitos fundamentais, Jorge Reis Novais<sup>46</sup> é adepto de uma teoria externa mitigada, que reconhece papel à ponderação, na solução de conflitos entre Direitos. O mesmo autor defende que não é possível que a Constituição consiga prever todas as possibilidades de colisões de Direitos e entre Direitos e bens constitucionalmente relevantes, no entanto, é possível identificar limites às restrições – legalidade, proporcionalidade, igualdade, não retroatividade – e que dificilmente se poderia estabelecer hierarquias *prima facie* entre Direitos, mas que é possível, a partir do Judiciário, estabelecer *standards* para soluções de casos, identificando casos que se aproximam e se distinguem, tentando estabelecer determinadas preferências, que exigiriam maior argumentação para serem afastadas nos casos concretos.

Por fim, importa pontuar que entende-se positivo o fato de no Brasil não haver a restrição explícita, mas deve-se entender que existem parâmetros para ponderação que estão na Constituição e que funcionam como limites dos limites.

---

<sup>44</sup> ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público), p.117.

<sup>45</sup> ÁVILA, Humberto. **Teoria dos Princípios**. 18. ed. São Paulo: Malheiros, 2018, p.173.

<sup>46</sup> NOVAIS, Jorge Reis. **As Restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição**. Coimbra: Coimbra Editora, 2003, p.83.

Nesta dissertação, interessa a análise do direito fundamental à privacidade e, para sua abordagem, é importante conhecer como se dá a proteção de dados com vistas a assegurar este direito. Assim, inicia-se abordando a evolução da proteção de dados na legislação europeia tendo em vista que a recente legislação brasileira que dispõe sobre a proteção aos dados é bastante similar à *General Data Protection Regulator* (GDPR) adotada atualmente na Europa.

## 1.2 A EVOLUÇÃO DA PROTEÇÃO DE DADOS E PRIVACIDADE NA LEGISLAÇÃO EUROPEIA

Na Europa, a norma atual, que entrou em vigor no dia 25.05.2018, é o Regulamento (EU) 2016/679 – conhecido como *General Data Protection Regulator* (Regulamento Geral da Proteção de Dados).

É necessário esclarecer que, desde 4.05.2016, o Regulamento (UE) 2016/679 já está substituindo a Diretiva 1995/46 e os países-membros tiveram prazo até 25.05.2018 para adequar os seus ordenamentos jurídicos ao novo documento<sup>47</sup>.

Como transcorreram cerca de 20 anos entre a Diretiva e o Regulamento e houve significativo desenvolvimento tecnológico nesse interregno (a ponto de modificar as relações entre particulares e entre esses e os Estados), a atualização normativa foi fundamental para garantir a tutela da proteção de dados pessoais dos europeus. Algumas mudanças estão elencadas a seguir:

[...] a consagração do “direito a ser esquecido” [grifo do autor] nos termos ao Art.º17º; a preocupação e protecção acrescida em torno do tratamento de dados pessoais que envolvam crianças, só valendo a sua licitude mediante o preenchimento do(s) requisito(s) [grifo do autor] de maior de 16 anos, ou, na sua falta, mediante a autorização pelos titulares das responsabilidades parentais, conforme Art. º8/1; o direito de portabilidade dos dados e o direito de oposição [grifo do autor] nos termos dos Arts. 20 e 21 do Regulamento [...]º48.

Quanto à aplicação territorial do Regulamento, verifica-se a ampliação da

---

<sup>47</sup> CASTRO, Nuno Teixeira. Um novo quadro legal europeu em matéria de proteção de dados vislumbrando o Mercado Único Digital para a Europa. **Diário Insónias**. [S.l.], 11.05.2016. Disponível em: <http://www.insonias.pt/um-novo-quadro-legal-europeu-materia-proteccao-dados-vislumbrando-mercado-unico-digital-europa/amp/>. Acesso em: 20 Fev. 2020.

<sup>48</sup> Ibidem.

abrangência para as empresas no art. 3º do RGPD que preceitua que suas regras se aplicam ao tratamento de múltiplos dados pessoais realizado em contextos diversos no território da UE, independentemente desse tratamento ser feito dentro ou fora da União. Igual aplicação ocorrerá para os indivíduos. Nesse sentido, Lemoalle e Carboni acrescentam que o RGPD também pode ser aplicado ao:

[...] tratamento de dados pessoais de titulares residentes no território da União Europeia, estejam estes localizados fisicamente dentro ou fora da União, que venha a ser feito por alguém que não esteja localizado na União, quando as atividades de tratamento estiverem relacionadas à oferta de bens ou serviços a esses titulares de dados pessoais, tais como, vendas online por meio de uma plataforma de *e-commerce*, direcionamento de anúncios publicitários veiculados em uma rede social, prestação de serviço de *cloud computing* e uma infinidade de atividades proporcionadas, sobretudo, por aplicações de Internet<sup>49</sup>.

Além das modificações expostas, destacam-se as ações adotadas pela Comissão Nacional de Proteção de Dados de Portugal nas seguintes áreas temáticas:

(i) informação aos titulares dos dados, (ii) exercício dos direitos dos titulares dos dados, (iii) consentimento dos titulares dos dados, (iv) dados sensíveis, (v) documentação e registro de atividades de tratamento, (vi) contratos de subcontratação, (vii) encarregado de proteção de dados, (viii) medidas técnicas e organizativas e segurança do tratamento, (ix) proteção de dados desde a concessão e (x) avaliação de impacto e notificação de violações de segurança<sup>50</sup>.

A primeira medida relaciona-se com a informação aos titulares dos dados. Já a próxima regra versa sobre o exercício dos direitos e sobre a ampliação das garantias dos titulares dos dados, ao passo que na terceira posição, encontram-se mudanças no consentimento dos titulares dos dados. Assim, devem ser verificadas a forma e as circunstâncias em que o consentimento dos titulares foi obtido, tendo em vista que se constitui em uma base legal para tratar os dados pessoais.

<sup>49</sup> LEMOALLE, Edouard; CARBONI, Guilherme. **Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil**. JOTA. [S.l.], 12.02.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018>. Acesso em: 23 Fev. 2020.

<sup>50</sup> COMISSÃO Nacional de Proteção de Dados. **10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados**. [S.l.], 28.01.2017. Disponível em: [https://www.cnpd.pt/bin/rgpd/10\\_Medidas\\_para\\_preparar\\_RGPD\\_CNPd.pdf](https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPd.pdf). Acesso em: 23 Fev. 2020.

Complementarmente, o regulamento amplia a definição de consentimento e inclui novas condições para que este seja obtido, motivo pelo qual é necessário constatar se o consentimento obtido por aquele que irá tratar os dados atende às novas exigências. Caso não seja assim, é necessária a obtenção de novo consentimento junto àqueles que detêm a titularidade dos dados, consoante o RGPD, pois, ao contrário, o tratamento de dados passa a ser ilícito em razão da ausência de base legal. Também, maior atenção deve ser dedicada ao consentimento dos menores (ou de seus representantes legais), levando-se em conta as especificidades das exigências referentes a este efeito<sup>51</sup>.

O conceito de dados sensíveis foi ampliado e outra novidade é a (quase total) equiparação entre o fornecedor e a empresa terceirizada que realiza o tratamento de dados pessoais. No sentido da regra anterior, a próxima inovação refere-se aos contratos de subcontratação de serviços, pois, estes, prestados no âmbito de tratamentos de dados pessoais devem ser revistos com vistas a identificar se contam com todos os elementos que o regulamento exige<sup>52</sup>.

O encarregado da proteção de dados assume relevância na transição da Diretiva 1995/46 para o Regulamento (UE) 2016/679 e foram regulamentadas as medidas técnicas, organizativas e segurança do tratamento com vistas a confirmar um estágio de segurança afeto ao tratamento adequado, que assegura a confidencialidade e a integridade dos dados, além de prevenir a destruição, perda e modificações, sejam elas acidentais ou ilícitas ou mesmo, a divulgação e acesso aos dados sem que estes sejam autorizados<sup>53</sup>.

A penúltima regra alterada correlaciona-se com a proteção de dados desde a concessão e com a avaliação de impacto e, por derradeiro, a última norma versa sobre notificação de violações de segurança.

---

<sup>51</sup> COMISSÃO Nacional de Proteção de Dados. **10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados**. [S.l.], 28.01.2017. Disponível em: [https://www.cnpd.pt/bin/rgpd/10\\_Medidas\\_para\\_preparar\\_RGPD\\_CNPD.pdf](https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf). Acesso em: 23 Fev. 2020.

<sup>52</sup> Ibidem.

<sup>53</sup> Ibidem.

Por fim, tem-se que o RGPD mostra-se necessário, eis que as inovações tecnológicas alteraram as relações sociais entre os sujeitos existentes (pessoas, empresas e nações), de modo que a legislação deve se adequar ao novo contexto fático.

Nessa esteira, segundo Guidi<sup>54</sup>, o RGPD inovou ao regulamentar procedimentos de avaliação de impacto sobre a privacidade, conhecidos como *Privacy Impact Assessments*, estes já adotados na esfera de autorregulamentação do modelo norteamericano, mas agora transpostos como mecanismos de aplicação cogente. Dentre tais procedimentos estão a elaboração de registro de tratamento de dados pelos responsáveis a serem submetidos à aprovação da autoridade de controle; bem como a consolidação dos instrumentos de *privacy by default* e *privacy by design* como exigências às empresas - ao construir seus produtos - planejar seus serviços e conduzir os processos de coleta e compartilhamento de dados, atuarem de modo a preservar ao máximo a privacidade dos usuários. Concomitantemente à ampliação das responsabilidades, o RGPD também previu incentivos aos responsáveis pelo tratamento de dados pessoais que se destacarem pelo zelo na aplicação dos mecanismos de proteção da privacidade dos seus usuários, mediante a criação de “selos” e sistemas de certificação das empresas comprometidas com os objetivos do regulamento.

### 1.3 A EVOLUÇÃO DA PROTEÇÃO DE DADOS E PRIVACIDADE NA LEGISLAÇÃO BRASILEIRA

A preocupação com o direito à privacidade, segundo Silva<sup>55</sup> teve início nos EUA, em 1890, quando na universidade de Harvard, passou-se a falar em direito de ficar sozinho e de direito ao esquecimento (*right to be let alone*).

---

<sup>54</sup> GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. 2017. Disponível em: <https://itsrio.org/wpcontent/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 23 Fev. 2020.

<sup>55</sup> SILVA, Alexandre Assunção. **Sigilo das Comunicações na Internet**. Curitiba: Juruá Editora, 2017, p.25.



Não há dúvidas de que a Internet trouxe e traz benefícios a todos, pois a grande maioria das tarefas desempenhadas, seja no trabalho ou em âmbito doméstico demanda o uso de tecnologias para tornar mais céleres processos que antes eram feitos manualmente. Diante das facilidades, surgem novas práticas ilícitas que tem como principal instrumento o computador associado à Internet, o que significa que os crimes já existentes estão sendo aperfeiçoados conforme será visto a seguir.

Ante a esta nova realidade que convencionou-se chamar de globalização, as comunidades em todo o mundo passaram a atuar no espaço cibernético, também chamado de ciberespaço, e, inevitavelmente, mudou para esse ambiente, indivíduos de índoles diversas, inclusive os criminosos.

A lei mais importante sobre crimes cibernéticos é o Marco Civil da Internet – MCI, que traz princípios, garantias, direitos e deveres para os internautas no Brasil, originada no PLC n. 2.126/2011, em 26.10.2011.

O projeto inicial do MCI buscou apresentar normas claras sobre os direitos, deveres, garantias e princípios para uso da Internet no Brasil. A proposta estabeleceu deveres e responsabilidades que devem ser exigidos dos prestadores de serviços, deixando claro o papel a ser exercido pelo poder público referente ao desenvolvimento do potencial social da rede.

Havia a necessidade de se defender alguns fundamentos para que a Internet no Brasil fosse preservada como um espaço dinâmico e de colaboração. Assim, como lembra Malaquias<sup>56</sup>, qualquer iniciativa de regulamentação posterior deve observar as diretrizes e os princípios eleitos como fundamentais, a exemplo da liberdade de expressão, privacidade, além do respeito aos direitos humanos.

As interpretações judiciais à época negligenciaram os princípios fundamentais e a arquitetura da Internet, levando o Comitê Gestor da Internet no Brasil (CGI.br) a editar, no ano de 2009, as “Diretrizes para o Uso e Governança da

---

<sup>56</sup> MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova: A Investigação Criminal em Busca da Verdade**. 2. ed. Curitiba: Juruá Editora, 2015, p.224.

Internet no Brasil”, em que foram delineados os dez princípios fundamentais para regulamentar a Internet, levando em consideração a harmonia dos preceitos constitucionais para assegurar o adequado funcionamento tecnológico no mesmo compasso exigido pela sociedade cibernética pátria, amplamente analisado anteriormente por esta pesquisa.

Outro importante projeto votado e aprovado foi o PLC 89/03(PL 84/99), apresentado em 13.11.2003 (Dep. Luiz Piauhyllino), que se transformou na Lei 12.737, de 30.11.2012, tipificando crimes informáticos e modificando o Código Penal. Esses dispositivos foram incluídos no Capítulo VI, que regulamenta os crimes contra a liberdade individual e, a seu turno, estão inseridos na Seção IV, onde encontram-se tipificados os crimes contra a inviolabilidade dos segredos.

Nesse projeto, a invasão de sistemas no sentido de obter segredos comerciais e industriais ou conteúdos de caráter privado, utilizando-se de técnicas remotas não autorizadas e violando mecanismos de segurança, tem a previsão da pena de reclusão de 6 meses a 2 anos e multa. Traz como agravante a hipótese de o criminoso divulgar, comercializar ou transmitir a terceiros os dados obtidos ilegalmente.

A invasão de dispositivo ou rede local com o objetivo de destruir ou modificar dados ou informações, além de instalar vulnerabilidades para obtenção de vantagens ilícitas ou apenas por vandalismo, foi penalizada com 3 meses a 1 ano de detenção e multa. Foi enquadrado no mesmo crime o indivíduo que produzir, oferecer, distribuir, vender ou divulgar programa de computador com a finalidade de executar crimes cibernéticos em computadores, *smartphones*, *tablets* ou outros dispositivos informacionais e em redes locais.

Segundo o autor do referido projeto, essa estruturação de tipos preenche a omissão atual na lei penal. Entretanto, seu mais ferrenho opositor, o Deputado Federal Eduardo Azeredo (PSDB-MG), relator de outro projeto (PLC n.84/1999) com características bastante diferentes, faz denúncia contra o casuísmo governamental afirmando que o governo, durante muito tempo, foi omissos sobre o tema e que devido o vazamento das fotografias da atriz Carolina Dieckmann, foi votado às

pressas um projeto que não foi sequer discutido em nenhuma comissão. Essas declarações são bastante significativas para demonstrar e ilustrar a importância que os parlamentares têm atribuído ao tema da cibercriminalidade.

Até 2012, quando se conseguia chegar ao cibercriminoso, eram utilizadas as leis já existentes para punir os crimes cometidos. Ainda não existiam mecanismos legais específicos para punir os autores de crimes cometidos pela internet. Assim, um criminoso que viesse a roubar informações de um determinado internauta usando de astúcia ou beneficiando-se da boa fé da vítima, poderia ser enquadrado, por exemplo, no crime de estelionato (art. 171<sup>57</sup> do CP).

Com o vazamento de fotos sensuais da atriz Carolina Dieckman em outubro de 2012 na Web, a ex-presidente, Dilma Rousseff sancionou duas leis que alteraram o Código Penal Brasileiro para estabelecer os crimes virtuais e suas respectivas sanções.

A Lei Carolina Dieckman (12.737/2012) e a Lei Azeredo (12.735/2012) entraram em vigor no dia 02 de abril de 2013 no Código Penal Brasileiro com o fito de tipificar diversas condutas no ambiente virtual.

No Brasil, em consequência do crescente número de usuários da Internet, urgente se fazia sua regulamentação e, em tal realidade, se deu a gênese do MCI, com a Lei nº 12.965/2014, que estabeleceu princípios, garantias, direitos e deveres que deveriam ser observados no uso da Internet no Brasil. Esta legislação busca, além da garantia dos princípios dos usuários, como sua privacidade, respeito aos direitos humanos e o exercício da cidadania nos meios digitais, o estabelecimento das diretrizes relacionadas à exploração comercial e governamental desse espaço digital.

Iniciada pelo Projeto de Lei 2.126, de 2011, pelo Poder Executivo, a Lei 12.965/14, antes de sua sanção, foi motivo de inúmeras controvérsias. Cuidando de temas como neutralidade de redes, armazenagem dos registros de conexão, guarda

---

<sup>57</sup> “Art. 171- Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. Pena- reclusão, de 1 (um) a 5 (cinco) anos, e multa.”

do registro das aplicações de Internet, privacidade, função social da rede, responsabilidade por material infringente, armazenamento de dados no País e atendimento à legislação nacional, dentre outros pontos, surgiram debates em demasia, dos quais participaram usuários, provedores de conexão e de conteúdo nacionais e internacionais, detentores de direitos autorais e o governo.

Referente à garantia da privacidade dos usuários da Internet, a nova lei trouxe algumas certezas que até então ensejaram dúvidas, tanto aos que se consideravam atingidos em sua dignidade no mundo virtual, como também para os operadores do Direito.

Neste trilhar, a Lei 12.965/14 consolidou a ideia de que os direitos constitucionais, como o de inviolabilidade da intimidade e da vida privada (art. 7º, inc.I), inviolabilidade de informações e direito à informação (art. 7º, incs. II e VI), são válidos também para o mundo virtual. Dessa forma, dispõe o Capítulo II, que trata dos direitos e garantias dos usuários, especificando a matéria da privacidade:

Art. 8º - A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que: I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil<sup>58</sup>.

De efeito, percebe-se que uma atenção maior aos direitos concernentes à vida privada do usuário foi positivada no ordenamento jurídico brasileiro. Ainda restam, entretanto, diversos questionamentos quanto aos limites de invasão da privacidade, principalmente quando se discutem relações trabalhistas, até mesmo pelo fato de o legislador não ter como prever todas as novas situações deparadas pelos empregadores e empregados todos os dias.

Ademais, o legislador buscou a proteção da vida privada dos usuários da Internet também em outros pontos. Exemplo está no caput do art. 10, da Lei

---

<sup>58</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 25 Fev. 2020.

12.965/14, que tem o intuito de proteger a privacidade no tocante a guarda e disponibilização de registros de conexão, acesso e de dados pessoais, exprimindo assim:

A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas<sup>59</sup>.

Em tal circunstância, o cidadão teria como limitar as informações que ele permite que tornem públicas, ainda que em detrimento da sua privacidade. “Trata-se da autodeterminação informacional fundada na perspectiva de que o próprio usuário deve ter controle sobre as suas informações pessoais, autodeterminando-as”<sup>60</sup>.

Como se pode notar, mesmo em meio aos embates travados para a aprovação da nova lei esta abrangeu diversos conteúdos, alterando normas, bem como as relações entre usuários e empresas da área. Até a aprovação do marco civil, as inúmeras incertezas jurídicas quanto à matéria barravam direitos e garantias constitucionais, quando ligadas ao mundo virtual. Era, portanto, necessária uma regulamentação para a Internet que limitasse, não somente, os poderes das empresas, mas, também, dos governos sobre os usuários, dando oportunidade à implantação de um modelo distinto de gerenciamento para a grande rede.

Foi neste contexto que surgiu a Lei Geral de Proteção de Dados (LGPD). A Lei Geral de Proteção de Dados (Lei 13.709/2018) ingressa tardiamente no ordenamento pátrio, porque somente após mais de quinze anos da criação da Rede Ibero-americana de Proteção de Dados – RIPD, talvez porque o Brasil integra somente como país observador. Entretanto, essa Lei geral de proteção de dados teve sua tramitação relativamente rápida no Poder Legislativo nacional, ingressando no final de maio de 2018 e sendo sancionada em agosto do mesmo ano. A rapidez

---

<sup>59</sup> BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 25 Fev. 2020.

<sup>60</sup> RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.267.

dessa tramitação deveu-se aos ataques cibernéticos ocorridos recentemente em diversas redes privadas e públicas, especialmente em anos anteriores.

A finalidade da LGPD é a tutela da privacidade, pois neste contexto dominado pelas tecnologias informativas os riscos de invasão da esfera particular do indivíduo se acentuam, tornando a esfera da privacidade mais vulnerável a invasões indevidas e injustificadas.

Sobre a abrangência do direito à proteção de dados pessoais, apresentam-se as seguintes condições:

[...] (a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos ou privados; (b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; (c) o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; (d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados; (e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados<sup>61</sup>.

Questão importante é a delimitação da titularidade do direito à proteção de dados pessoais. Parece não haver dúvidas em relação à condição da pessoa natural como destinatária imediata desta forma de tutela. Porém, não são estes os únicos merecedores de proteção em relação aos seus dados, pois, como bem explana Sarlet, Marinoni e Mitidiero<sup>62</sup>, as pessoas naturais (e inclusive os entes despersonalizados) também são merecedores de atuarem como destinatárias das normas sobre a adequada gestão de dados.

Quanto à aplicação desta Lei, se prevê que esta ocorre em qualquer operação em que os dados pessoais são tratados por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, país de sua sede, ou país onde os dados estejam localizados. Entretanto, tal aplicação observa o aspecto da territorialidade quando alcança somente: 1) as operações realizadas no território nacional (critério objetivo); 2) se a operação de tratamento for realizada fora do território nacional, mas os dados sejam de pessoas que se encontram no território

---

<sup>61</sup> SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2014, p.473-474.

<sup>62</sup> Ibidem.

nacional (critério subjetivo); ou 3) independentemente do local do tratamento desses dados, a coleta destes tenham ocorrido em território nacional (critério objetivo)<sup>63</sup>.

Faz-se necessário observar que quando a Lei estabelece que “consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta”<sup>64</sup>, o aspecto da localização do indivíduo, mediante os protocolos de internet, conhecidos como a sigla IP<sup>65</sup> (*Internet Protocol*), é um referencial necessário para se aferir se houve ou não essa violação dos direitos tutelados pela LGPD.

Em uma sociedade na qual as informações se tornam a riqueza mais importante, a tutela da privacidade com base nos dados pessoais que transitam na internet contribui de forma decisiva para o equilíbrio de poderes. Poder que migrou da mão do soberano e constitucionalmente foi sendo atribuído ao povo. Por isso, o fim da privacidade não representaria somente um risco para as liberdades individuais, seria efetivamente conduzir ao fim da democracia<sup>66</sup>.

A LGPD buscou estabelecer um sistema de proteção formado por representantes do Estado e da sociedade civil. Entretanto, a efetividade dessa proteção vai depender do quanto o indivíduo esteja informado de que instrumentos dispõem para que sua privacidade não seja violada sem que saiba, por meio das diversas interfaces tecnológicas que o atual mundo informatizado oferece para o consumo de uma maneira geral e a comodidade.

Assim, essa proteção prevista na Lei visa à proteção da privacidade que é direito da personalidade. Nesse âmbito, a dignidade da pessoa é o princípio de valor

---

<sup>63</sup> MÊLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019, p. 83.

<sup>64</sup> § 1º do art. 3º da Lei 13.709/2018.

<sup>65</sup> [...] é o principal protocolo de comunicação da Internet. É o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores. Pacotes são os blocos de informações enviados na Internet e podem ser considerados como as cartas enviadas pelo serviço de correios. Informação disponível em: <https://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html>. Acesso em: 25 Fev. 2020.

<sup>66</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.269.

absoluto, conforme argumentado por Alexy<sup>67</sup> ao elaborar as equações para solução da colisão de princípios. Chega a ser afirmado por Rodotà<sup>68</sup> que a proteção de dados constitui não apenas um direito fundamental entre muitos outros: é o mais expressivo da condição humana contemporânea, e que essa proteção pode ser compreendida como a junção de direitos que fundamentam a cidadania do novo milênio.

Portanto, em âmbito mundial, o cenário que se apresenta com avanço tecnológico, diante de um mundo globalizado, onde as mais diversas informações pessoais transitam em velocidade que pode chegar à da luz, seja por um ideário de crescimento econômico, seja por motivos de segurança, todas as fontes do Direito têm um papel fundamental nessa era chamada de pós-modernidade. Os reflexos desta dinâmica são imediatos no Direito, pois este deve mostrar-se capaz de responder às novidades propostas pela tecnologia com a reafirmação de seu valor fundamental – a pessoa humana e sua dignidade.

No entanto, a proteção à pessoa humana e à privacidade mostra-se um desafio frente à evolução tecnológica. É o que será discutido a seguir.

#### 1.4 A INFLUÊNCIA DA TECNOLOGIA E A PRIVACIDADE NA SOCIEDADE ATUAL

Na atualidade, a importância (ou até mesmo indispensabilidade) da Internet requer a adequação de inúmeros conceitos ao seu ambiente, entre os quais a privacidade.

Fortes estabelece quatro direitos-base a título de direitos de privacidade na Internet (originalmente, *Internet Privacy Rights*): “o direito de navegar pela internet [sic] com privacidade; o direito de monitorar quem monitora; o direito de deletar os dados pessoais; o direito a uma identidade online”<sup>69</sup>.

---

<sup>67</sup> ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público), p.94.

<sup>68</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.21.

<sup>69</sup> FORTES, Vinícius Borges. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016, p.183.



Os conceitos de privacidade e de proteção de dados pessoais na Internet possuem muitos aspectos, resultado das várias possibilidades de uso desse instrumento, o que cria um desafio legal para a correta tutela dos interesses dos indivíduos.

Sendo o direito à privacidade corolário da dignidade humana e um direito fundamental de primeira dimensão, sua tutela de modo adequado é elemento indispensável em um Estado democrático de direito. Nesse sentido, o ciberespaço tem enorme potencial para a participação política e atividades comunitárias. Longhi<sup>70</sup> salienta que a privacidade na Internet é um pressuposto de um sistema democrático deliberativo por dois grandes motivos. O primeiro diz respeito à guarda dos dados pessoais como forma de evitar hierarquizações e discriminações com base em informações pessoais. O segundo, a restrição da autonomia privada do indivíduo frente ao abuso de poderes públicos e privados quando detentores de informações pessoais.

Mas estes não são os únicos problemas jurídicos em torno da proteção da privacidade dos cidadãos em um sistema democrático. O primeiro deles é o da definição de sua abrangência. Isto porque, há, no ocidente, dois grandes sistemas que se dedicam à garantir a privacidade: liberdade e dignidade. O da liberdade, oriundo dos países da common law, tutela a privacidade como uma espécie de liberdade pública abrangente, que justifica a não intervenção de terceiros na esfera de decisão do indivíduo. Já a privacidade como dignidade é uma característica dos países da tradição jurídica continental, restringindo-se à proteção da intimidade e vida privada dos indivíduos<sup>71</sup>.

Restringindo-se às TICs, leciona Rodotà<sup>72</sup> que o direito à privacidade hoje ganha novos contornos, dando margem à existência de um direito autônomo dele decorrente, a proteção dos dados pessoais. Embora ambas façam alusão à proteção

---

<sup>70</sup> LONGHI, João Victor Rozatti. **Processo Legislativo Interativo**. Curitiba: Juruá Editora, 2017, p.136.

<sup>71</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.139.

<sup>72</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.19.

da dignidade humana, os dados pessoais tutelam um bem jurídico diverso da intimidade. Enquanto um cuida do “corpo físico” o outro cuida do “corpo eletrônico”. Ou seja, os dados, quando analisados e disponibilizados em conjunto, permitem que se formem perfis a serviço tanto do mercado como do Estado. Algo que põe em risco todos os outros direitos e garantias fundamentais.

E o tema da proteção dos dados pessoais se depara com novos desafios diuturnamente. Exemplificativamente, a questão do *big data*, o problema do direito ao esquecimento, o “consentimento” do cidadão em disponibilizar informações relevantes em sites de redes sociais, cujos provedores “praticamente sabem o que pensamos”<sup>73</sup>.

Assim, o avanço tecnológico, além de trazer diversos benefícios para a sociedade, também trouxe algumas preocupações. A inserção de dados pessoais na rede, o posterior desejo de torná-los indisponíveis, bem como as novas formas como estas informações têm sido utilizadas, acenderam a discussão sobre o direito de os usuários terem protegida a sua privacidade, além dos seus dados pessoais.

Cada dia mais o acesso a dados pessoais contendo informações sensíveis do indivíduo não depende do acesso ao seu *smartphone* ou dispositivo pessoal, mas pode ser obtido através do consentimento de provedores considerados como “terceiros” nesta relação (no direito norte-americano conhecido por *third-party providers*), o que na prática representa um controle cada vez menor de seus dados pessoais<sup>74</sup>.

Desta maneira, episódios como o escândalo de espionagem<sup>75</sup> praticado pela *National Security Agency* (NSA) norte-americana em todo o mundo, são apenas uma amostra do ambiente de vigilância constante a que se está submetido hoje, no entanto, não se pode dizer que é sempre que esta vigilância está a serviço do direito

---

<sup>73</sup> FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. **University of Pennsylvania Law Review**, v. 163, n. 327, January, 2015, p.409.

<sup>74</sup> Ibidem, p.379.

<sup>75</sup> Ressalte-se que as pessoas envolvidas neste caso estão no Brasil e se envolveram em casos de violações de aplicativo telefônico de autoridades em território brasileiro e encontraram abrigo no STF. Destaque-se também que um dos países que é acusado de fazer espionagem por diversos outros é a China.

à informação, mas que é possível que, neste caso, em razão dos excessos observados, ocorre violação do direito à privacidade.

Porém, não é sempre que se pode falar em direito à privacidade. Exemplo disso são algumas operações realizadas em território nacional em que boa parte se dá através e-mail, plataformas e aplicativos que encontram-se localizados em território americano. A título de exemplificação, toda vez que alguém usa sua conta do gmail, yahoo ou apple, se submete às regras americanas. Assim, foi promulgado pelos EUA, o *Cloud Act* que tem o objetivo de agilizar o acesso a informações eletrônicas coletadas e armazenadas pelos EUA para prestadores globais que atuam investigando crimes graves, a exemplo do terrorismo, cibercrime e exploração sexual<sup>76</sup>.

Esta é uma iniciativa importante, pois, as dificuldades para conseguir cooperação internacional com vistas a angariar evidências/provas eletrônicas, na maioria das vezes em tempo exíguo, motivou a edição do *Cloud Act*, segundo que viabiliza acordos e parcerias entre as nações, em busca de maior eficiência em face da criminalidade grave. Trata-se de um marco porque garante privacidade, ao estabelecer critérios para se ter acesso aos dados sobre empresas globais de tecnologia.

Segundo Steinmetz “há colisão de direitos fundamentais quando, in concreto, o exercício de um direito fundamental por um titular obstaculiza, afeta ou restringe o exercício de um direito fundamental de outro titular”<sup>77</sup>.

Asseverou Doneda<sup>78</sup> que ao se estabelecer uma tutela de dados pessoais, devem também ser levadas em consideração situações acerca da liberdade de informação e da liberdade de expressão. Indubitavelmente, a proteção de dados pessoais poderá ter reflexos com outras atividades, a exemplo da

---

<sup>76</sup> ROSA, Alexandre Moraes; VIEIRA, Marília Raposo. **Cloud Act**: Quando a investigação se dá nas nuvens americanas. 2019. Disponível em: <https://www.conjur.com.br/2019-nov-22/limite-penal-cloud-act-quando-investigacao-nuvens-americanas>. Acesso em: 9 abr. 2020.

<sup>77</sup> STEINMETZ, Wilson. **Colisão de direitos fundamentais e princípio da proporcionalidade**. Porto Alegre: Livraria do Advogado, 2001, p.139.

<sup>78</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.146-147.

segurança pública, ou com o fluxo de informações que acompanha o comércio. Com efeito, a questão deve ser observada a partir do seu elemento básico, que é a informação.

O conteúdo da informação pode abranger tanto os fenômenos da natureza quanto fenômenos sociais e políticos. Estes últimos envolvem assuntos em que a pessoa é o principal protagonista. Na perspectiva de abordagem dessa seção, e para delimitar a abordagem, este tópico se ocupará da situação tradicional de conflito entre o direito à privacidade do indivíduo e o direito à informação decorrente da liberdade de expressão e comunicação, que atualmente não fica resumida aos dos profissionais da comunicação. Serão também pontuados alguns aspectos sobre a possibilidade de a pessoa divulgar fatos da sua vida privada, com intuito de se tornar famosa e provavelmente ter retorno financeiro, como alguns recursos tecnológicos favorecem.

O avanço tecnológico, especialmente com a internet, proporcionou uma revolução na maneira como a informação passou a ser produzida, pesquisada e utilizada. Cebrián<sup>79</sup> aduz que a combinação da informática com o sistema de telecomunicações e os grandes bancos de dados ou os meios de informação proporciona o funcionamento de redes de transmissão de maneira informal, e não necessariamente hierarquizada, nas quais os consumidores da informação são, em muitas circunstâncias, seus próprios provedores e emissores. Isso fez com que a notícia pudesse ser produzida e circulada não só pelos veículos e instituições tradicionais de comunicação, mas também por qualquer pessoa que tiver acesso a ferramentas tecnológicas de comunicação que utilize a internet.

Nesse contexto, a maneira pela qual a informação é produzida e veiculada na sociedade globalizada e da informação, mudou significativamente em relação à década passada. A comunicação é o processo indispensável nessa dinâmica da trajetória da informação. Conforme acentuado por Cebrián<sup>80</sup>, o âmbito fundamental da comunicação, pública ou privada, refugiou-se nos lares, porque se

---

<sup>79</sup> CEBRIÁN, Juan Luis. **A Rede**: como nossas vidas serão transformadas pelos novos meios de comunicação. Lisboa: Summus, 1999, p.13.

<sup>80</sup> Ibidem, p.14-15.

tornou possível realizar inúmeras atividades por intermédio de um PC em casa; desenvolveram-se novas relações entre os usuários e os próprios meios ou seus representantes quando, por exemplo, a relação de comunicação entre as pessoas passou a se estabelecer à distância, mesmo que as pessoas nunca tenham tido contato pessoal; os modelos sociais viram-se substituídos, e alguns valores em voga foram aniquilados para dar lugar a outros, a exemplo da possibilidade de qualquer pessoa se tornar conhecida publicamente, por meio das redes sociais, a depender do que esteja disposta a expor na rede.

Associada a essa realidade, a cultura da sociedade brasileira acerca da notícia ocupa-se mais pelas notícias envolvendo as pessoas, especialmente fatos da vida pessoal. As notícias mais veiculadas, por despertar maior interesse social e, conseqüentemente, audiência, sendo lucrativas para as emissoras, são aquelas que dizem respeito à privacidade. As incursões dos paparazzi fazem com que os veículos de comunicação especializados tenham garantido seu produto de venda, a vida privada e, algumas vezes a intimidade pessoal.

Nether<sup>81</sup> expõe que os defensores da divulgação de determinados fatos, ainda que envolvam a privacidade do indivíduo sustentam suas razões no exercício do direito à liberdade de expressão e comunicação, as quais promoverão a informação. Por outro lado, os defensores da manutenção de sigilo de determinados fatos sustentam suas razões na proteção dos direitos da personalidade, especialmente nos elementos que compõem a privacidade.

As possibilidades de obtenção dos mais diversos tipos de informações passaram a ser incomensuráveis. Assim, associando a grande quantidade de informações que podem ser obtidas, mediante os recursos tecnológicos contemporâneos, e a facilidade com que as informações pessoais possam se tornar conhecidas, seja pelo exercício do direito à liberdade de expressão e comunicação, ou manifestação do pensamento, seja pela vulnerabilidade de determinados bancos de dados em que há informações pessoais, surge o inevitável conflito do direito

---

<sup>81</sup> NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018, p.133.

fundamental à informação com o direito fundamental à privacidade<sup>82</sup>.

Porém, faz-se necessário ressaltar também que o que vai ser determinante para se estabelecer a amplitude do direito à informação, na relação com a privacidade, basicamente será a condição pessoal de pessoa pública ou famosa, bem como o que alguém, deliberadamente, torna público mediante os recursos de acesso à informação e comunicação contemporâneos oferecem, a exemplo dos *blogs* e páginas de redes sociais. Sobre a circunstância de ser a pessoa famosa ou pública, a jurisprudência pátria majoritária sinaliza para uma menor privacidade. Entretanto, sem que haja um total afastamento desse direito fundamental.

Diante desse panorama e tendo em vista o propósito do estudo, as possibilidades de violação da privacidade aumentaram substancialmente com o avanço tecnológico, ainda que a pessoa não se exponha deliberadamente. Determinados atos da intimidade e da vida privada, discretamente ou cuidadosamente, realizados no espaço público, atualmente podem ser capturados pelos mais diversos recursos tecnológicos informacionais. A imagem da pessoa, da casa, as comunicações de todos os tipos, mediante correspondência tradicional (carta) ou eletrônica (*e-mail*), telefônica (voz ou mensagens eletrônicas), de dados, e telegráfica passaram a ser registrados, arquivados, tratados e com possibilidade de serem manipulados em locais desconhecidos, tendo em vista a estrutura mundial de rede que a internet inaugurou.

Informações sobre a vida privada ou da intimidade da pessoa, portanto, dados da privacidade podem ser acessadas sem a autorização, ou sequer, o conhecimento pelo titular. Essa circunstância ocorre, tendo em vista a maneira como informações relacionadas à pessoa podem ser capturadas, classificadas, arquivadas e tratadas, pelas tecnologias informacionais.

---

<sup>82</sup> NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018, p.134-135.

Nesse sentido, acentua Rodotà<sup>83</sup> seguindo os desenvolvimentos da tecnologia, percebe-se que a própria noção de arquivo, de banco de dados tende a se tornar obsoleta, e que a nova fronteira certamente não se encontra nos computadores pessoais, mas assume uma dimensão bem maior, de rede. Por isso, não é apenas o cenário tecnológico que se modifica, também muda profundamente o ambiente jurídico-institucional. Essa situação é acentuada quando estas informações pessoais estão deixando de ser arquivadas exclusivamente nos equipamentos pessoais, e estão migrando para o chamado arquivamento em nuvem<sup>84</sup>.

Esse rol de direitos fundamentais<sup>85</sup> foi posto na Constituição para assegurar o estabelecimento de um regime democrático de direito. Observa-se que aspectos da privacidade são uma constante. Porém, em determinadas circunstâncias a liberdade de informação e o direito à privacidade poderão conflitar, conforme será visto mais adiante.

Segundo Robl Filho<sup>86</sup>, para a concretização desses direitos exigidos pela ética pós-moralista, gerou a necessidade de a doutrina e jurisprudência brasileiras desenvolverem instrumentos jurídicos compatíveis com as necessidades cotidianas e contemporâneas desses direitos, onde há colisões, negociações e até renúncia<sup>87</sup> de alguns desses direitos fundamentais. Sobre a questão da renúncia tácita, Stefano Rodotà faz a seguinte observação:

Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo

---

<sup>83</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.24.

<sup>84</sup> Termo utilizado para denominar os serviços oferecidos pelos provedores de acesso em que disponibiliza espaço para arquivamento de dados, dispensando que o usuário archive no HD do PC. Exemplo significativo desse serviço: Google Drive. Mais informações em: [https://www.google.com/intl/pt\\_PT/drive/start/index.html](https://www.google.com/intl/pt_PT/drive/start/index.html). Acesso em: 27 Fev. 2020.

<sup>85</sup> Proteção da imagem da pessoa, da inviolabilidade da casa, e das comunicações de todos os tipos, e o sigilo de dados.

<sup>86</sup> ROBL FILHO, Ilton Norberto. **Direito, Intimidade e Vida Privada**: Paradoxos jurídicos e sociais na sociedade hipermoderna. Curitiba: Juruá, 2008, p.37.

<sup>87</sup> Exemplo básico dessa renúncia ocorre quando a condição para se usufruir de determinadas utilidades oferecidas pela internet é o cadastramento pessoal com fornecimento de dados pessoais, até então considerados cadastrais e juridicamente possível de conhecimento público na era imediatamente anterior à atual sociedade da informação.

escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações<sup>88</sup>.

Tem-se assim a circunstância em que direitos fundamentais passam a ser renunciados de maneira tácita, o que desafia uma análise de aspectos sobre a interpretação, associados à questão do conflito entre princípios. Nessa perspectiva, aduz Dimoulis e Martins<sup>89</sup> que as principais ferramentas para decidir sobre casos de conflitos de direitos fundamentais são: a interpretação sistemática da Constituição e a utilização do critério da proporcionalidade.

---

<sup>88</sup> ROBL FILHO, Ilton Norberto. Op. cit., p.37.

<sup>89</sup> DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 3. ed. rev. atual. e ampl. São Paulo: RT, 2011, p.120-129.



## CAPÍTULO 2

### AS NOVAS TECNOLOGIAS E DITAMES ATUAIS

Este capítulo trata das novas tecnologias frente aos ditames atuais. Assim, explica o atual uso da inteligência artificial nos tempos modernos; o uso de *Big Dates*; o lado positivo e o negativo das novas tecnologias; e, por fim, expõe sobre os serviços tecnológicos que integram o tratamento de dados.

#### 2.1 A INTELIGÊNCIA ARTIFICIAL NOS DIAS ATUAIS

O termo Inteligência Artificial correspondente à habilidade de um programa de computador de desenvolver funções e raciocínio típicos da mente humana<sup>90</sup>. A IA é uma disciplina debatida simultaneamente entre cientistas e filósofos os quais se manifestam, por sua vez, não só sobre os aspectos teóricos, como também práticos que o termo comporta. Associado ao debate da mente e da sua relação com o cérebro, encontramos outras manifestações, que interferem no resultado prático que se pretende obter por meio da IA, dentre os quais a consciência e a cognição. A relação dual entre mente e cérebro, na sua unidade, ao lado da ideia de que se possa considerar um como manifestação do outro, divide os pesquisadores.

Influenciados pelo contexto niilista ou relacional entre mente e cérebro, os mais notórios profissionais buscaram de forma intrínseca em seus estudos a evidência mais simples de suas teses. A problemática mente-cérebro é confrontada nesta pesquisa com aspectos externos à cognição, permeados pelas instituições, pela sociedade e pela ordem jurídica dos povos.

O conteúdo científico da IA é extraordinariamente amplo e multifacetário. Mas, em todas as etapas do seu desenvolvimento, seu estado foi determinado, em última instância, por demandas objetivas de acesso àquela força que se chama

---

<sup>90</sup> BITTENCOURT, G. **Inteligência artificial**: ferramentas e teorias. 2. ed. Florianópolis: Editora da UFSC, 2001, p.16.

cérebro humano. É estimulado por ele que ditas demandas se aprofundem nas indispensáveis premissas materiais para o trânsito de sua formação interior e superior<sup>91</sup>.

As teses fundamentais e teóricas que tornam possível a sustentação acerca de uma firme base científica o estudo da IA estão sintetizadas no conjunto de dados concretos que põem a descoberto o cérebro humano. Ao longo do tempo, essa conclusão não significou em absoluto a negação do significado dos fatores objetivos para o avanço da IA. Desprendida da compreensão exata do papel do cérebro humano nas suas relações fundamentais com a noção de mente, a IA avançou, progressivamente com o intuito de atender aos reclamos da sociedade<sup>92</sup>.

O objetivo central da IA é promover a criação de teorias e modelos de capacidade cognitiva e prática na implementação de sistemas computacionais, baseados nesses modelos. Os modelos implementados em um computador de modo a os tornar autônomos, análogos à ação inteligente do comportamento psíquico do homem, constitui o objetivo ainda por escrever da IA.

O impetuoso processo de formação do sistema computacional na sua importante parte de IA é o substrato físico, no qual essa última se materializará. E esse substrato normalmente é o computador digital. Desde o início da história dos computadores, com os primeiros mecanismos artificiais construídos para marcar o tempo ou para simular o comportamento de animais ou de pessoas, os chamados autômatos foram, ao longo do tempo, desenvolvidos como relógios, depois máquinas de calcular e, finalmente, computadores<sup>93</sup>.

A ideia desses autômatos sempre esteve ligada à sua capacidade de realizar tarefas surpreendentes, de engajar pessoas em programas de IA. Essa tarefa titânica de substituir o cérebro humano por mecanismos engenhosos vem

---

<sup>91</sup> BITTENCOURT, G. **Inteligência artificial**: ferramentas e teorias. 2. ed. Florianópolis: Editora da UFSC, 2001, p.18.

<sup>92</sup> McDOWELL, J. **Mente y mundo**. Trad. Miguel Angel Quintana. Salamanca: Ediciones Sígueme, 2003, p.33.

<sup>93</sup> SCHMIDT, Eric; COHEN, Jared. **A nova era digital**: como será o futuro das pessoas, das nações e dos negócios. Tradução de Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013, p.51.

encontrando resistência, em razão da capacidade única do ser humano em definir-se, intencionalmente, pela consciência. A intencionalidade da consciência seria o fator determinante do processo de desenvolvimento da IA. Essa é a concepção desenvolvida por Searle<sup>94</sup> em seu Naturalismo Biológico. Segundo ele, desenvolver consciência exige intencionalidade que só o cérebro humano é capaz de realizar.

Serve aos mesmos fins de limitar e impedir a concepção mais ampla de uma consciência não humana, por ausência de intencionalidade, a existência em particulares setores práticos de aplicação, de regras legais que impeçam, igualmente, agora por força de lei, a criação de um mecanismo com a mesma capacidade de um juiz de produzir um julgamento.

A principal peculiaridade da Tese de Searle<sup>95</sup> de que a consciência não poderia existir em outro lugar senão no cérebro humano é, na concepção especificamente comparativista, uma limitação por natureza. Ao lado dessa concepção, sublinhamos outra: a da limitação por força de lei. A lei pode, independentemente da capacidade de sua realização, proibir que algo mesmo possível possa existir.

Provavelmente existam ações que o cérebro realiza que não podem ser descritas em termos computacionais, a exemplo dos sentimentos de felicidade, amor, vontade, entendimento etc., talvez não possam ser enquadrados apenas a imagens e procedimentos.

Em relação às conjecturas sobre as possibilidades de um computador no futuro possuir uma mente similar à humana, Penrose<sup>96</sup> classifica alguns níveis computacionais e os relaciona com as atividades cerebrais. Assim, identifica quatro distintos pontos de vista extremos e possíveis para os limites da IA. São eles:

---

<sup>94</sup> SEARLE, J.R. **O mistério da consciência**. Trad. André Yuji Pinheiro Uema e Vladimir Safatle. São Paulo: Paz e Terra, 1998, p.53.

<sup>95</sup> Ibidem.

<sup>96</sup> PENROSE, R. **Shadows of the mind: a Search for the Missing Science of Consciousness**. Oxford: University Press, 1994, p.45.

- A - Todo o pensamento reduz-se à computação e a experiência da consciência pode ser produzida através da computação apropriada.
- B - A consciência decorre de processos físicos que ocorrem no cérebro e, embora elas possam ser simuladas em computador, as simulações por si só não produzem a consciência.
- C - As atividades físicas do cérebro que produzem a consciência não podem ser simuladas através de algoritmos computacionais.
- D - A consciência nem se reduz à computação nem às atividades físicas do cérebro e não pode ser explicada cientificamente<sup>97</sup>.

O modelo *D* é o domínio do misticismo e da religiosidade. Como a tentativa é a busca de caminhos através da ciência, tal ponto deve ser completamente rejeitado em face da incompatibilidade com a metodologia científica.

O extremo oposto é a possibilidade *A*. Seus adeptos são os partidários da IA forte, também podendo ser identificados como funcionalistas, que parece ser, neste contexto, um tanto nebuloso. Alguns outros defensores de *A* se diferenciam na forma como interpretam o significado de “consciência”. Alguns nem permitem que haja um fenômeno como “consciência” em tudo, enquanto outros aceitam a existência desse fenômeno, mas o consideram como apenas algum tipo de propriedade emergente que se relaciona a um determinado grau suficiente de sofisticação envolvido nos procedimentos computacionais.

O argumento operacional pregado pelo modelo *A* parece apresentar deficiências, pois se todas as manifestações externas de um cérebro consciente, incluindo respostas ao questionamento contínuo, podem de fato ser completamente imitadas por um sistema sob o controle computacional, então seria plausível aceitar que suas manifestações internas de consciência deveriam ser também consideradas em associação com tal simulação.

A aceitação desse tipo de argumento relaciona-se basicamente com o teste de Turing<sup>98</sup> que, em essência, distingue *A* e *B*. Segundo *A*, um robô controlado

---

<sup>97</sup> ROSA, Luiz Pinguelli. **Introdução ao problema da Inteligência Artificial e da mente**. 2019. Disponível em: <https://cosmosecontexto.org.br/introducao-ao-problema-da-inteligencia-artificial-e-da-mente>. Acesso em: 8 mar. 2020.

<sup>98</sup> O teste de Turing é um teste da capacidade de uma máquina para exibir um comportamento inteligente. O teste foi introduzido por Alan Turing em 1950, em seu artigo ‘*Computing Machine ryand Intelligence*’ e consistia em um modelo matemático, baseado em autômatos finitos, composto por um grupo finito de símbolos, um número finito de estados e uma fita de comprimento ilimitado dividida em pequenas células organizadas em sequência. A máquina de Turing foi um

por qualquer computador que, depois de um questionamento sustentado, se comporta de forma convincente, como se possuísse consciência, deve ser considerado realmente consciente. De acordo com o ponto de vista *B*, um robô poderia perfeitamente se comportar exatamente como uma pessoa consciente pode se comportar sem realmente possuir qualquer qualidade mental.

*A* e *B* permitiriam que um robô controlado por computador poderia se comportar de forma convincente como uma pessoa consciente faz, mas o modelo *C*, por sua vez, não admite a possibilidade de uma simulação totalmente eficaz de uma pessoa consciente através de um robô. Assim, de acordo com *C*, a falta real de consciência do robô deve finalmente se revelar, após um interrogatório suficientemente longo. De fato, *C* é muito mais próximo do modelo *A* sob este ponto de vista do que *B*. Penrose<sup>99</sup> considera o modelo *B* o “senso científico comum”.

Também é referido como a IA fraca. Da mesma maneira que *A*, afirma que todos os objetos físicos do mundo devem se comportar de acordo com uma ciência que, em princípio, permite que possam ser computacionalmente simulados. Por outro lado, nega veementemente a alegação operacional que uma coisa que se comporta externamente como um ser consciente deve necessariamente ser consciente em si. Isso vai ao encontro da declaração de Searle<sup>100</sup> que afirma que uma simulação computacional de um processo físico é uma coisa muito diferente do processo propriamente dito. Por exemplo, a simulação em computador de um furacão não é certamente um furacão.

O modelo *C* é o defendido por Penrose<sup>101</sup>. Declara que existem manifestações externas de objetos conscientes (por exemplo, o cérebro) que diferem das manifestações externas de um computador, os efeitos externos da consciência não podem ser adequadamente simulados computacionalmente. Nesta

---

artefato tão grandioso do ponto de vista da evolução da ciência, que, mesmo sendo apenas teórica é considerada como um dos fundamentos da Ciência de Computação.

<sup>99</sup> PENROSE, R. **Shadows of the mind**: a Search for the Missing Science of Consciousness. Oxford: University Press, 1994, p.45, p.48.

<sup>100</sup> SEARLE, J.R. **O mistério da consciência**. Trad. André Yuji Pinheiro Uema e Vladimir Safatle. São Paulo: Paz e Terra, 1998, p.59.

<sup>101</sup> PENROSE, R. **Shadows of the mind**: a Search for the Missing Science of Consciousness. Op. cit., p.64..

abordagem, talvez um novo entendimento seja de fato necessário, em uma área intermediária e sutil que conecte os domínios macro e micro do universo que nos cerca.

Talvez existam outras possibilidades de combinações dos modelos apresentados ou que possam estar localizadas entre tais modelos, como se fossem gradações dos mesmos. Existe até um ponto de vista que poderia ser considerado como uma combinação de *A* e *D* (ou talvez *B* e *D*). De acordo com essa visão, a ação do cérebro é realmente a de um computador, mas um computador de tão extrema complexidade que a sua simulação estaria além das capacidades do ser humano e da ciência contemporânea.

O programa ELIZA, criado em 1996, possui funcionamento similar ao teste de Turing. Foi criado por Joseph Weizenbaum, professor de ciência da computação do MIT<sup>102</sup>. O software simula uma espécie de psicólogo que somente faz ecoar a própria questão do paciente sem substanciais interpretações. Como relata Murray<sup>103</sup>, algum tempo após a criação do programa surge um relato de um caso em que um cientista teria deixado uma versão de ELIZA funcionando em seu computador e o presidente da empresa em que trabalhava teria conversado com o programa acreditando estar falando com o cientista. A conversa vem abaixo reproduzida:

VP: Do you think that I can use the computer this morning?  
 ELIZA: Why do you ask?  
 VP: I might be able to make some additional telcomp sales.  
 ELIZA: Why aren't you so sure?  
 VP: My prospective costumers have never seen a demonstration of the system.  
 ELIZA: Does this mean very much to you?  
 VP: Of course it does.  
 ELIZA: You seem very positive about that.  
 VP: This is ridiculous.  
 ELIZA: What do you mean this is ridiculous?  
 VP: Is there any reason why I can't use the computer now?  
 ELIZA: Tell me more about the prospective costumers.  
 VP: Please dial me up on 491-1850<sup>104</sup>.

<sup>102</sup> MURRAY, J. **Hamlet on the holodeck**: the future of narrative in cyberspace. Cambridge/Londres: MIT, 1997, p.71.

<sup>103</sup> Ibidem, p.71-72.

<sup>104</sup> VP: Você acha que posso usar o computador esta manhã?  
 ELIZA: Por que você pergunta?

Como o presidente se esqueceu de colocar um ponto final no diálogo, o computador parou de responder, fazendo com que o chefe, nervoso, telefonasse para o cientista para esclarecer o ocorrido.

O importante no caso relatado, e no próprio teste de Turing é a possibilidade de o ser humano acreditar na inteligência da máquina a ponto de confundi-la com a inteligência de uma pessoa. Assim, parece ainda uma missão insólita separar inteligência artificial de inteligência racional, criatura e criador e estas dificuldades encontram reflexos na área do Direito, ainda subjetivo, mas que frente à vida que tem ganhado as máquinas, vê-se instado a tornar-se artificial.

Nesse contexto, surgem alguns questionamentos: poderão as máquinas responder juridicamente tal como o fazem os homens? Poderão os homens ser julgados por uma máquina dotada de IA?

Estas são questões que há alguns anos pareciam fantasiosas, mas que frente ao galopante desenvolvimento tecnológico, já merecem ser pensadas.

Dito isto, passa-se à análise sobre as implicações do uso de *Big Datas* cujo objetivo é fazer com que dados imperfeitos e complexos sejam transformados em conhecimento útil.

## 2.2 O USO DE *BIG DATAS*

A tradução literal de *Big Data* é “megadados, grandes dados”. Assim, a expressão *Big Data* significa “grande volume de dados”, dados estes que podem ser estruturados ou não, que incentivam o cruzamento de informações que permitem a

---

VP: Talvez eu faça algumas vendas *telcomp* adicionais.

ELIZA: Por que não tem certeza?

VP: Os prováveis clientes ainda não viram uma demonstração do sistema.

ELIZA: Isso é importante para você?

VP: Claro que sim.

ELIZA: Você parece certo disso.

VP: Isso é ridículo.

ELIZA: Como assim?

VP: Existe algum motivo para que eu não use o computador agora?

ELIZA: Me fale mais sobre os prováveis clientes.

VP: Por favor me ligue no telefone 491-1850.

tomada de decisões estratégicas pelas empresas<sup>105</sup>.

Sendo um método de análise de dados inteligente e eficaz, as empresas têm usado o *Big Data* para obter informações válidas, que lhe serão benéficas de alguma maneira. Assim, as empresas empregam os resultados obtidos para compreender melhor o mercado, lançar novos produtos e serviços, e responder às mudanças de padrões quase que instantaneamente<sup>106</sup>.

Além das empresas, os governos também têm se beneficiado das possibilidades de *Big Data*, sendo-lhes possível conhecer percepções e comportamentos de determinadas comunidades, através da análise de dados digitais. Isso pode ser de grande importância na administração de cidades, área da saúde, segurança pública e em vários outros setores que interessam aos cidadãos e políticos, a exemplo do uso de *Big Data* em campanhas eleitorais<sup>107</sup>.

O termo “big data” começou a aparecer nos dicionários durante a última década, mas o próprio conceito existe desde pelo menos a Segunda Guerra Mundial. Mais recentemente, a conectividade sem fio, a Internet 2.0 e outras tecnologias tornaram o gerenciamento e a análise de grandes conjuntos de dados uma realidade<sup>108</sup>.

O tratamento dos dados bem como os serviços que o integram será melhor detalhado na seção 2.5 deste capítulo.

## 2.3 O LADO POSITIVO DAS NOVAS TECNOLOGIAS

A tecnologia pode ser compreendida como a utilização de métodos baseados no conhecimento técnico ou científico, com o objetivo de desenvolver

---

<sup>105</sup> DOYLE, Daniella. **O que é *Big Data* e por que é tão valioso para sua empresa?** 2020. Disponível em: <https://www.siteware.com.br/gestao-estrategica/o-que-e-big-data/>. Acesso em: 8 Mar. 2020.

<sup>106</sup> FREITAS JR., José Carlos da Silva; MAÇADA, Antônio Carlos Gastaud; OLIVEIRA, Mirian et al. *Big Data e gestão do conhecimento: definições e direcionamentos de pesquisa*. **Revista Alcance**, v.23, n.4, p.529-546, 2016.

<sup>107</sup> SCHMIDT, Eric; COHEN, Jared. **A nova era digital: como será o futuro das pessoas, das nações e dos negócios**. Tradução de Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013, p.66.

<sup>108</sup> Ibidem.



ferramentas que possibilitem ou aperfeiçoem a execução de uma tarefa específica<sup>109</sup>.

Após a Revolução Agrícola e a Industrial, o mundo perpassa agora, a passos acelerados, a Revolução Digital, ocorrida nas telecomunicações, de uma forma geral, surgindo novas tecnologias a todo instante, moldando a sociedade de acordo com essa perspectiva de rapidez e economia na transmissão de informações. Trata-se de um momento de explosão de mídias digitais, uso do computador pessoal, da internet, dos *tablets* e *smartphones*, que permitem transmissão de dados em tempo real para várias pessoas ao mesmo tempo. Potencializou-se, assim, a sociedade da informação, marcada por pessoas conectadas a todos os acontecimentos ao seu redor, responsáveis por revolucionar a forma de se comunicar e de se relacionar; um mundo em que existem inúmeros amigos mas também inimigos virtuais<sup>110</sup>.

A comunicabilidade tornou-se múltipla, e evidenciou-se uma contínua progressão no desenvolvimento das telecomunicações. No passado, observa-se que as interações entre os sujeitos ocorriam pelo mecanismo das cartas, posteriormente, evoluíram para o telefone, e, atualmente, conversa-se instantaneamente por um visor do computador ou de um celular. O sistema educacional alterou-se, o professor e os livros não são mais as fontes exclusivas de conhecimento, as aulas começaram a acontecer em uma modalidade de educação a distância (EAD), e o quadro preto/verde, que também já foi branco, poderá ser substituído por um quadro interativo digital, que permite a apresentação de materiais dinâmicos e a simulação de fenômenos naturais e realidades virtuais. Palestras podem ser reproduzidas ao mesmo tempo para diversos ambientes, bastando, para esse intento, a interligação de todos os usuários, estejam eles numa sala comercial, auditório ou em suas residências. O indivíduo tornou-se mais autodidata.

No universo da política, a Internet também produziu mudanças, e atualmente os candidatos podem interagir com seus pretensos eleitores nas páginas

---

<sup>109</sup> MARQUES, J; SILVA, M.F. **O Direito na Era digital**. Porto Alegre: Livraria do Advogado Editora, 2012, p.117.

<sup>110</sup> Ibidem.

de campanha eleitoral no ambiente da *web*. O ato de votar foi alterado, o voto na cédula de papel foi substituído pelo voto digital, modernidade que garantiu que os resultados das eleições sejam computados logo após o término da votação e quase imediatamente se tenha acesso aos novos representantes do povo no governo. A própria relação do Estado com a população é intermediada pelas Tecnologias da Informação e Comunicação (TICs) – vive-se a era do governo eletrônico.

Neste contexto, como afirma Alexandre Morais da Rosa<sup>111</sup>, a função das TICs, providas de IA, apresenta-se como revolucionária. O antigo modelo de decisão fundamentado em capacidades individuais requer a conjugação de mecanismos tecnológicos aptos a ampliar o horizonte de credibilidade, volume, dentre outros critérios, fazendo com que o *Big Data* se torne um auxiliar importante.

Alexandre José Mendes, Alexandre Morais da Rosa e Izaías Otacílio da Rosa<sup>112</sup> prevêem que em um futuro não muito distante, até mesmo as sentenças serão proferidas com o uso da IA, especialmente quando trata-se de demandas repetitivas, sendo este um recurso mais eficaz se comparado à capacidade de um único indivíduo para exarar-las.

Diante do avanço constante das biotecnologias e da chamada IA, o questionamento do indivíduo acerca de sua “humanidade” torna-se recorrente. Quando é possível (ou iminentemente possível) que uma máquina supere ou se iguale em desempenho ao seu criador ou que o homem possa ser clonado e seu código genético alterado, o sentido de humano tende a sofrer um deslocamento. Isto porque sendo o indivíduo o criador da máquina não é de se estranhar que ele a tenha construído à sua imagem e semelhança. O que se questiona é o quão semelhante ao homem essa máquina se tornou (ou se tornará), a ponto desta semelhança implicar em algum estágio de independência evolutiva da criatura com relação ao seu criador.

---

<sup>111</sup> ROSA, Alexandre Morais da. A questão digital: o impacto da inteligência artificial no Direito. **Revista de Direito da Faculdade Guanambi**, Guanambi, v.6, n.2, p.1-18, 2018, p.4.

<sup>112</sup> MENDES, Alexandre José; ROSA, Alexandre Morais da; ROSA, Izaías Otacílio da. Testando a *Methodology Multicriteria Decision Aid – Constructivist* (MCDA-C) na construção de algoritmos de apoio à estabilidade das decisões judiciais. **Revista Brasileira de Direito**, Passo Fundo, v. 15, n. 2, p. 281-305, Mai-Ago, 2019, p.6.

## 2.4 O LADO NEGATIVO DAS NOVAS TECNOLOGIAS

É bem conhecido o efeito principal da IA: as práticas computacionais, com o potencial para a simulação de comportamento inteligente. Disso poder-se-ia indagar se o surgimento desse engenho atenderia aos importantes aspectos da organização social, da democracia e da liberdade.

A primeira indagação seria quanto aos limites territoriais da soberania nacional. O espaço cibernético difere do espaço físico, pois sua arquitetura tem como principais características, a maleabilidade e flexibilidade. Qualquer um pode redefinir códigos e interagir, o que o converte em um objeto inacessível e refratário às regras legais que levem em conta o elemento territorial para determinar os inúmeros aspectos jurídicos da questão.

Em segundo lugar, o tempo virtual na sua aceleração de massiva difusão imprimiria um estado de coisas divorciado das categorias comunitárias e naturais que configuram o tempo real. Do mesmo modo, a privatização dos espaços virtuais e a sua inevitável vulnerabilidade. Ademais, o paradigma judicial contemporâneo da decisão judicial daria margem a que fosse substituído pelo dilema da melhor solução inteligente – já que pode ser mais de uma. Uma *Lex informatica*<sup>113</sup> ao invés de uma *Lex fundamentalis*<sup>114</sup> seria a nova referência dos estudos jurídicos<sup>115</sup>.

O princípio da vinculação à lei e ao direito seria a única fonte para os julgamentos, certamente. Mas, e os contornos que a equidade oferece? Se as regras de experiência comum e especial seriam beneficiadas, assim como os fatos notórios, o princípio da livre convicção motivada seria possível?

É pertinente recordar o exemplo da literatura jurídica da estação de trem que proibia animais no seu interior, mas que, por exercício de equidade, deixava o cego com um cão condutor passar, ao lado de outra estação de trem que permitia o acesso de animais, mas não que um urso fosse também levado. Em ambos os

---

<sup>113</sup> Lei informática.

<sup>114</sup> Lei fundamental.

<sup>115</sup> MARQUES, J; SILVA, M.F. **O Direito na Era digital**. Porto Alegre: Livraria do Advogado Editora, 2012, p.101.

exemplos, prevaleceu a decisão, norteadada pelo bom senso, que ponderou as regras existentes para torná-las adequadas e próprias aos fins que lhe deram causa. É por isto que se diz que o direito deve servir ao homem e não ser servido por ele.

As mudanças estruturais de uma nova sistemática de julgamentos propiciariam pouca margem para caracterizar, na amplitude que assegura a Constituição da República, o conceito remoto e distante de justiça. Mais ainda, suscitam discussões sobre a ética e os valores jurídicos imbricados na aplicação da justiça no controle social na era cibernética.

A concepção atual de Justiça é provecta e desde a época Aristóteles era observada, pois o modelo era colocado como um risco à sua não obtenção, tendo em vista a condição relativa da personalidade humana consoante ilustra Gilissen, “Aristóteles é um dos primeiros a admitir a relatividade humana: uma forma de governo pode ser boa ou má conforme o grupo social ao qual se destina”<sup>116</sup>.

Os resultados da modernidade sinalizam desilusão, no entanto, ao mesmo tempo, apresentam sinais de superação frente ao desenvolvimento da sociedade e dos aspectos que a envolvem. Segundo Baumann<sup>117</sup>, na maior parte de sua história, a modernidade viveu na autoilusão, sem se preocupar com os muitos males advindos de suas consequências, o que aponta para a necessidade de superar a cegueira moderna, a fim de que as condições da pós-modernidade possam processar-se de uma forma mais positiva.

A tecnologização do Judiciário precisa atingir seu núcleo operacional, contribuindo com o aperfeiçoamento de seus resultados em todos os aspectos, no entanto sem ameaçar o desenvolvimento e as conquistas historicamente obtidas. Com isso, o paradigma da modernidade passa a ter como marca o uso da tecnologia em todos os meios, devendo fazer com que a nova espécie de conhecimento e inteligência estejam presentes em todos os momentos e espaços de maneira

---

<sup>116</sup> GILISSEN, J. **Introdução histórica ao direito**. Tradução A. M. Botelho Hespanha e L. M. Macaísta Malheiros. 4. ed. Lisboa: Fundação Calouste Gulbenkian, 2003, p.77.

<sup>117</sup> BAUMAN, Z. **O mal-estar da pós-modernidade**. Tradução Mauro Gama; Cláudia Martinelli Gama. Rio de Janeiro: Zahar, 1998, p.76.

positiva, inclusive na difícil e importante missão de conduzir a sociedade para muito além das condições exigidas por sua limitação cognitiva.

O sentido através do qual a história da humanidade se desenvolve deixa claro que os conhecimentos encontram-se todos mesclados entre si e, por esse motivo, a sistematização tecnológica da Justiça é mais que a aceitação das novas tendências: é a prova viva de que a realidade é constituída de partes totalizantes e não de fatias do saber.

O conhecimento nada mais é do que o exercício das adversidades cognitivas e é dessa relação que as pessoas devem participar a fim de que seja possível validar as normas reguladoras das realidades estabelecidas. Desta forma, a transposição desta estrutura para uma linguagem torna-se legítima para a resolução de conflitos e, conseqüentemente, sua pacificação social, através de uma linguagem tecnológica.

A relação entre o homem e a máquina assemelha-se a vias paralelas, ou seja, não se cruzam, são graus cognitivos que não esbarram. Por isso, a IA, mais do que ajudar o indivíduo, tem como objetivo assegurar-lhe uma via mais célere e segura em um cenário ultramoderno, que demanda maior precisão e objetividade<sup>118</sup>.

A vivência dessa nova etapa requer a aceitação da concomitância de vidas, de consciências, de motivações e outras faculdades que tornam únicas cada uma das estruturas cognitivas bem como suas respectivas finalidades.

Não há porque então questionar o determinismo das máquinas, nem inquirir se elas podem ou não alcançar o mesmo dinamismo do homem ou a previsibilidade da Justiça. O determinismo está aliado à ética humana, responsável por ordenar o funcionamento do sistema, já que a consciência da máquina está pré-determinada por sua programação e, portanto, detém um potencial ilimitado.

---

<sup>118</sup> SANTOS, Fábio Marques Ferreira. **O limite cognitivo do poder humano judicante a um passo de um novo paradigma cognitivo de justiça**: poder cibernético judicante – o direito mediado por inteligência artificial. 668f. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, PUC-SP, 2016, p.168.

Pode-se dizer que hoje a inclusão digital é um direito fundamental e que a segurança digital é um novo direito humano. Isto porque são poucas as ações cotidianas do homem que não requerem a informatização e apesar disso, a regulamentação ainda é deveras rudimentar.

Passou a vigorar em 2014 no Brasil a Lei 12.965, conhecida como o Marco Civil da Internet, que regula os direitos e deveres dos usuários da rede mundial de computadores.

A identificação dos criminosos virtuais é muito mais difícil do que a identificação de criminosos que cometem crimes típicos. Nesse cenário, a polícia científica ainda tem um longo caminho a percorrer. No entanto, é importante que sejam desenvolvidos meios para identificar os agentes que praticam delitos em meios digitais. É preciso também conhecer os tipos de crimes que são praticados nesse meio a fim de que sejam criadas leis específicas para delitos específicos, e não se use apenas a lei vigente de forma análoga. Segundo Carvalho:

[...] o espaço virtual possui características que demandam uma normatização própria, sob pena de eliminar a possibilidade de identificação dos infratores quando alguém tiver um direito violado, e ao mesmo tempo, de forma a respeitar os direitos fundamentais<sup>119</sup>.

O Marco Civil da Internet passou a regulamentar, no art. 10 sobre os registros de navegação, estabelecendo a regulamentação do provedor responsável no que tange à intimidade de dados, registros de conexão de usuários bem como o sigilo das informações armazenadas.

O artigo 14 dispôs que o provedor de conexão com a internet não pode armazenar registros de acesso a aplicações da *internet* assim como o provedor de aplicação de *internet* também não pode armazenar os registros de acesso sem a permissão do usuário, nem os dados pessoais que não sirvam ao fim para o qual se deu permissão, nos termos do artigo 16. No artigo 9º, §3º, “proíbe-se que os provedores de internet, gratuitos ou onerosos, ou aqueles responsáveis pela transmissão, comutação e roteamento de dados, realizem bloqueios, filtros ou

---

<sup>119</sup> CARVALHO, Ana Cristina Azevedo. **Marco Civil da Internet no Brasil**. São Paulo: Editora Alta Books, 2014, p.89.

análises de conteúdo dos pacotes de dados”<sup>120</sup>.

Outra questão que recebeu atenção do legislador foi o combate às ilicitudes civis e criminais cometidas sob o manto da privacidade na rede mundial de computadores. Se, pela ótica social, a *internet* torna possível, contatos interpessoais anônimos, pela ótica técnica, toda ação realizada na internet pode ser registrada pelos provedores de acesso e de conteúdo, o que viabiliza a identificação dos usuários. Desta forma, o artigo 13, *caput*, do Marco Civil da Internet demanda que os registros de conexão à internet sejam armazenados por um ano e, consoante o artigo 15, *caput*, o registro de acesso a aplicativos da internet por seis meses<sup>121</sup>.

Estas são conquistas importantes, mas insuficientes, pois, quando se pensa em IA, o que povoa o imaginário popular são situações improváveis e vistas somente em filmes de ficção científica, mas, o fato é que o uso de tecnologias para realizar tarefas antes realizadas apenas pelos seres humanos está cada vez mais presente no mundo real. Existe um grande horizonte para a disseminação da IA, inclusive na esfera legal e, conseqüentemente, muitos interesses e questões éticas em torno desta situação.

A título de exemplificação cita-se o caso de um rapaz que criou um *chatbot*<sup>122</sup> que conseguiu vencer mais de 150 mil multas de trânsito nas cidades de Londres e Nova Iorque, em 21 meses. O robô de IA é o DoNotPay<sup>123</sup>, com índice de aproveitamento 64%. O criador desta plataforma *online* já começou a desenvolver outras para esclarecer portadores do vírus HIV sobre seus direitos, auxiliar no pedido de indenizações por atrasos das companhias aéreas e uma plataforma para ajudar refugiados em pedidos de asilo. São plataformas voltadas para o bem, mas poderiam ser diferentes, o que demandaria uma resposta do direito, que, a seu turno, não estaria apto a fornecê-la em razão das lacunas na legislação.

---

<sup>120</sup> TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Revista USP**, São Paulo, v.30, n. 86, p. 269-285, Apr., 2016.

<sup>121</sup> Ibidem.

<sup>122</sup> Programa de computador que simula a conversa com um ser humano no diálogo com as pessoas.

<sup>123</sup> Robô que exerce funções de advogado e que ajuda motoristas a recorrerem de multas de trânsito.

Um exemplo negativo de danos causados pela IA foi a proposta da @TayandYou, que diz respeito a um perfil criado pela Microsoft no Twitter com estética própria, capacidade para sobre tudo e publicar textos e imagens. Através de algoritmos, o perfil aumentava seu vocabulário quando interagia com adolescentes. O objetivo era que esta experiência fosse aplicada também a outros projetos, no entanto o perfil, que conseguiu 70.000 seguidores, não ficou nem 24 h no ar, pois, algumas pessoas começaram a se comunicar com a Tay fazendo uso de vocabulários e comentários impróprios, e ela, a seu turno, absorveu o que recebeu dos humanos e fez declarações racistas e nazistas como: “Nós vamos construir uma muralha, e o México vai pagar por ela”; “o Bush arquitetou o 11/9 e Hitler teria feito um trabalho melhor do que o macaco que temos agora” e “Hitler estava certo, eu odeio judeus.” Este incidente poderia ter sido evitado se a Microsoft tivesse designado um moderador para aprovar os *tweets*<sup>124</sup>.

O estágio evolucionista a que se chegou é tão complexo, que já se fala em imortalização do homem através da máquina. Segundo Lemos<sup>125</sup>, Hans Moravec é o principal defensor do uso da tecnologia para imortalizar o sujeito. Defende o *download* da mente humana para o computador, o que significaria sua continuidade além da simples existência ao ser convertido em informação.

Não muito distante da realidade hoje conhecida, pode-se citar os robôs inteligentes que estão sendo utilizados para ensino, inspeção de linhas aéreas, tomada de decisões pelas organizações, distribuição de energia elétrica, triagem de pacientes em instituições de saúde, combate a incêndios, para fins de salvamentos nas praias, dentre muitas outras finalidades.

Imagine-se a hipótese de que por um erro de programação um desses robôs ao invés de salvar, acabe por concorrer para a morte da vítima que deveria ser salva?

---

<sup>124</sup> Denominação dada para as postagens feitas na rede social twitter.

<sup>125</sup> LEMOS, A. **Cibercultura**: tecnologia e vida social na cultura contemporânea. Porto Alegre: Sulina, 2002, p.72.



Assim, o que as máquinas podem fazer pelos seres humanos pode ser fantástico ou muito perigoso e é por isto que as consequências jurídicas da IA precisam ser consideradas e regulamentadas pelo Direito a fim de que o ser humano não fique à mercê das máquinas.

O fato é que se antes a máquina estava a serviço do indivíduo, agora está-se a caminhar para que o homem fique à serviço da máquina. Nesse contexto, há quem defenda que as chances do homem cometer erros é maior do que as máquinas. Não se discute a veracidade da assertativa, mas a questão é: o ser humano é passível de responsabilização na esfera jurídica, mas as máquinas ainda não. Essa é a questão que deve receber especial atenção do Direito.

Questões como a criação de uma personalidade jurídica para robôs inteligentes, criação de um fundo para garantir acidentes causados por robôs inteligentes, criação de um sistema de registro de robôs, criação de um código de ética para desenvolvedores de *softwares* e robôs dotados de inteligência e responsabilização dos criadores, empresas e usuários de robôs com IA precisam ser urgentemente pensados, tal como já tem sido proposto por alguns países como é o caso da União Europeia.

## 2.5 SERVIÇOS TECNOLÓGICOS QUE INTEGRAM O TRATAMENTO DE DADOS

Na primeira parte deste Capítulo foi destacado que as redes de informação organizadas pela internet proporcionam vantagens extraordinárias, como ferramentas de organização em virtude da flexibilidade e adaptabilidade, as quais são características essenciais para sobrevivência e prosperidade num ambiente de rápida mutação, como acontece com as tecnologias de informação<sup>126</sup>.

Nesse contexto, afirma Cebrián<sup>127</sup> que as novas tecnologias da informação, que proporcionam uma aceleração das mudanças em nossas sociedades, forçam a humanidade a adaptar-se às novas relações no espaço e no

---

<sup>126</sup> CASTELLS, Manuel. **A galáxia internet**: reflexões sobre a internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003. p. 7.

<sup>127</sup> CEBRIÁN, Juan Luis. **A Rede**: como nossas vidas serão transformadas pelos novos meios de comunicação. Lisboa: Summus, 1999, p.8.

tempo. A transparência e o acesso global à informação serão necessários nos próximos anos para as atividades interativas e a solidariedade mundial. Para que tais condições se concretizem deve haver uma reconciliação entre as perspectivas humanísticas e as científicas. Significa estabelecer um ponto de equilíbrio entre circunstâncias paradoxais, por exemplo, essa ampla possibilidade de obtenção de informações pela internet e a proteção da privacidade quando da utilização de recursos tecnológicos conectados à internet.

Como bem acentua Rodotà<sup>128</sup>, as tecnologias da informação e da comunicação podem tornar mais transparentes todas as atividades públicas ou privadas que afetem direitos fundamentais da pessoa. Tais tecnologias da informação e da comunicação oferecem grandes oportunidades para promover uma cidadania ativa. A passagem da comunicação vertical, típica dos meios de comunicação tradicionais de rádio e televisão, à comunicação horizontal, interativa, típica do que a internet proporciona, permite resgatar o cidadão da passividade de mero espectador ou consumidor de informações e produtos, transformando-o em “protagonista de um processo no qual desaparecem as distinções entre produtores e consumidores de informações”<sup>129</sup>.

Observa Cebrián<sup>130</sup>, a existência de um paradoxo nesse sistema atual de comunicação, o qual se presume ser participativo, universal e aberto, entretanto possibilita também um controle quase que total dos cidadãos. Há uma completa incerteza sobre se os bancos de dados nos quais se encontram registradas suas informações pessoais, profissionais e familiares não podem ser acessados pela rede, e violados pelos próprios responsáveis pela tecnologia ou manipulados por instituições públicas ou privadas que tenham interesses totalmente desconhecidos por quem seja alvo dessa incursão.

---

<sup>128</sup> RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**: A Privacidade Hoje. São Paulo: Renovar, 2008, p.159-161.

<sup>129</sup> Ibidem, p. 161.

<sup>130</sup> CEBRIÁN, Juan Luis. **A Rede**: como nossas vidas serão transformadas pelos novos meios de comunicação. Lisboa: Summus, 1999, p.88.

Aduziu Castells<sup>131</sup> que se esperava da internet um instrumento ideal para promover a democracia, tendo em vista sua característica de interatividade, o que tornava possível aos cidadãos solicitar informações, expressar opiniões e pedir respostas pessoais a seus representantes. Porém, diante da maneira como foi configurada, ou seja, como a internet e a rede de computadores em geral interconectaram países inteiros, de fato no mundo inteiro, as vias de comunicação para a invasão de sistemas de segurança são quase ilimitadas. Afirmo ainda que há uma eficaz contramedida que poderia reforçar a segurança por todo o sistema: a implantação da tecnologia avançada de criptografia<sup>132</sup> para organizações e as pessoas em geral.

Porém, surgiu o seguinte dilema: implantando a tecnologia avançada de criptografia aumentaria a segurança dessas comunicações, por outro lado, dificultaria a investigação de comunicações que pusessem em risco a segurança de um país ou países inteiros, a exemplo dos planos para cometimento de atentados terroristas, ou invasões de sistemas por *hackers*. Para isso, são criados os mais diversos dispositivos que consigam neutralizar o poder de criptografia nos softwares de uso dos cidadãos, sob o argumento da segurança. Assim, são ampliados os poderes das instituições de vigilância que agem sobre interceptação de conversas telefônicas e de tráfego de dados, como foi visto em relação ao sistema Echelon. Chega-se ao ponto de obrigar os provedores de serviços da internet a dispor de técnicas para o rastreamento de seus usuários, bem como impõem a notificação compulsória de identidade de usuários por solicitação de agências governamentais, numa variedade muito ampla de situações e em circunstâncias vagamente definidas<sup>133</sup>.

Diante desse quadro, como fica a situação do indivíduo que necessita ter sua privacidade protegida, para o seu desenvolvimento enquanto pessoa? Segundo

---

<sup>131</sup> CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p.128-131.

<sup>132</sup> O movimento de defesa da criptografia para as comunicações pela internet, como forma de garantir privacidade e escapar dos controles de governos e corporações é conhecido como Cypherpunks. O líder desse movimento é Julian Assange, criador e editor-chefe do WikiLeaks, grupo que revelou documentos secretos dos EUA.

<sup>133</sup> CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p.147.

Assange “a internet, nossa maior ferramenta de emancipação, está sendo transformada no mais perigoso facilitador de totalitarismo que já se viu. A internet é uma ameaça à civilização humana”<sup>134</sup>, afirma o editor, que as agências de espionagem dos EUA têm acesso a todos os dados armazenados na maior ferramenta de pesquisa e busca de informações na internet (*Google*)<sup>135</sup>, na atual maior rede social (*Facebook*)<sup>136</sup>, no mais utilizado site de compras (*Amazon*)<sup>137</sup>, e nas administradoras de cartão de crédito multinacionais. Afirma que se trata de uma militarização do ciberespaço, ao mesmo tempo que uma privatização da vigilância pessoal, por grandes corporações privadas e públicas. Aqui cabe lembrar o afirmado por Jochai Ben-Avie<sup>138</sup> acerca do percentual de empresas privadas que controlam a internet, e do aspecto da gratuidade de muitas informações e serviços oferecidos na rede mundial. Nesse cenário, alguma empresa ou grupo de empresas paga para que haja gratuidade por quem é usuário das mais diversas facilidades oferecidas, porém, devido a diversos interesses estratégicos de natureza econômica e, segundo Julian Assange, militar, o principal produto dessa rede é a pessoa e todas as informações que lhe digam respeito, muitas vezes fornecidas ingenuamente. Como adverte Cebrián<sup>139</sup> inexistente qualquer segurança em relação à privacidade na comunicação de dados, sejam eles de qualquer tipo: econômicos ou amorosos, exceto se forem utilizados sistemas de codificação e cifras, a chamada

---

<sup>134</sup> ASSANGE, Julian. **Cypherpunks**: Liberdade e o Futuro da Internet. São Paulo: Boitempo, 2013, p.25.

<sup>135</sup> Segundo o site RankBrasil, teve início em janeiro de 1996, por meio de um projeto universitário, é atualmente considerado a maior fonte de pesquisa do Brasil e também do mundo. Segundo dados divulgados pela própria empresa em agosto de 2012, em média, o Google rastreia diariamente 20 milhões de páginas e 30 trilhões de URLs. Por mês, são cerca de 100 bilhões de buscas feitas em todo o planeta. Disponível em: [http://www.rankbrasil.com.br/Recordes/Materias/068-/Google\\_E\\_O\\_Maior\\_Site\\_De\\_Buscas](http://www.rankbrasil.com.br/Recordes/Materias/068-/Google_E_O_Maior_Site_De_Buscas). Acesso em: 8 mar. 2020.

<sup>136</sup> Segundo informações publicadas pela Uol, o Facebook tem mais de 1 bilhão de usuários, com inserção em 213 países. Se o número representasse a população de um país, seria o terceiro maior do mundo (só perderia para China e Índia). Esse número de pessoas é equivalente ao triplo da população dos EUA. Disponível em: <http://tecnologia.uol.com.br/album/2012/08/03/maior-rede-social-do-mundo-facebook-tem-numeros-estrafanticos-conheca.htm#fotoNav=1>. Acesso em: 8 mar. 2020.

<sup>137</sup> Segundo informações publicadas pela Revista Exame Info. Disponível em: <http://info.abril.com.br/noticias/mercado/pesquisa-aponta-amazon-como-melhor-site-para-compras-online-2712-2012-10.shl>. Acesso em: 8 mar. 2020.

<sup>138</sup> Analista Sênior de Política de Acesso ([www.AccessNow.org](http://www.AccessNow.org)), uma ONG internacional que promove o livre acesso à internet como um meio de livre, completo e seguro participação na sociedade e na realização dos direitos humanos.

<sup>139</sup> CEBRIÁN, Juan Luis. **A Rede**: como nossas vidas serão transformadas pelos novos meios de comunicação. Lisboa: Summus, 1999, p.88.

criptografia. Uma das características do espaço em que a internet funciona é a facilidade com que qualquer pessoa pode ter violado algum direito pessoal ou patrimonial, não apenas quando está navegando por ele, mas, inclusive, quando está sem utilizá-lo.

Adverte também Freire<sup>140</sup> que a velocidade com que a tecnologia avança é superior à capacidade com que outros setores que a utilizam possam acompanhar, principalmente no sentido de compreender sua abrangência e direção. Cita a mais recente e promissora ferramenta de integração de todos os outros instrumentos de monitoramento da sociedade e, conseqüentemente, da pessoa, como câmeras, telefones celulares e demais instrumentos de comunicação existentes atualmente, denominada WiMAX<sup>141</sup>. Possibilitará uma solução completa para voz, dados, vídeo e segurança num só pacote. A grande vantagem de utilização, que seduz qualquer pessoa, sem perceber o nível de possibilidade de violação de sua privacidade, é a capacidade de acesso à internet de qualquer lugar, mesmo se locomovendo, sem a necessidade de fios, cabos, ou até antenas no local de onde estiver acessando.

Ainda nesse cenário, Magrani destaca o acrônimo IoT<sup>142</sup>, ressaltando que existem fortes divergências em relação ao conceito mas que “todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade”<sup>143</sup>.

Nesse contexto, cabe mencionar a ponderação de Rodotà<sup>144</sup> no sentido de que se mudada a perspectiva, nota-se que as várias possibilidades oferecidas pelas tecnologias da informação e da comunicação também possibilitam o

---

<sup>140</sup> FREIRE, Alexandre. **Inevitável Mundo Novo**: O Fim da Privacidade. São Paulo: Axis Mundi, 2000, p.156.

<sup>141</sup> Worldwide Interoperability for Microwave Access. A conhecida tecnologia 4G. Mais informações disponíveis em: <http://tecnologia.uol.com.br/especiais/ultnot/2005/12/29/ult2888u131.jhtm>. Acesso em: 8 mar. 2020. Trata-se da tecnologia considerada uma evolução sofisticada do Wi-Fi. Consiste num padrão aberto de conexão sem fio, certificado pelo IEEE – Institute of Electrical and Electronics Engineers, em que não é uma tecnologia que haja proprietário. Uma característica da estrutura em redes como analisado por Marilyn Ferguson.

<sup>142</sup> Internet of Things (internet das coisas).

<sup>143</sup> MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV, 2018, p.20.

<sup>144</sup> RODOTÀ, Stefano. **A Vida na Sociedade da Vigilância**: A Privacidade Hoje. São Paulo: Renovar, 2008, p. 165.

desenvolvimento de processos de manipulação e de controle em poder de grupos restritos, sejam privados ou públicos, desvirtuando completamente a possibilidade de participação mediante ação política do cidadão. Vê-se assim que coexistem em paradoxo, as tecnologias da liberdade de informação e participação com as tecnologias do controle. Conforme acentuado por Doneda,

[...] os efeitos das tecnologias informáticas penetraram de tal modo em várias instâncias da vida dos cidadãos, sejam estes usuários diretos ou não de computadores, que separar os fenômenos relativos à informática de outros tornou-se tanto impossível quanto irrelevante<sup>145</sup>.

As atividades que tais instituições realizam, a depender da sua natureza, basicamente, têm relação com o comércio, a comunicação, a educação, a pesquisa, a prestação jurisdicional, dentre outras. Porém, todas essas atividades devem ser pautadas nas necessidades primordiais do ser humano para o seu desenvolvimento enquanto pessoa. Por isso, deve ser destacado que “a pessoa e sua dignidade são o valor e o princípio subjacente ao grande mandamento do respeito ao próximo [...] e está na origem dos direitos materialmente fundamentais e representa o núcleo essencial de cada um deles”<sup>146</sup>.

Constam no voto do relator da Comissão Especial constituída para apreciar o Projeto de Lei 2.126, de 2011<sup>147</sup>, que se estima existir 2 bilhões de terminais conectados à internet no mundo<sup>148</sup>. Em 2020, projeções são de que haverá 50 bilhões de terminais conectados. Tal projeto de lei apresentado pelo Poder Executivo em 24.08.2011 e transformado na Lei Ordinária 12.965/2014 visa estabelecer princípios, garantias, direitos e deveres para o uso da internet no país, trouxe as seguintes considerações:

---

<sup>145</sup> DONEDA, Danilo. **Da Privacidade à Proteção dos Dados Pessoais**. Rio de Janeiro: Renovar, 2006, p.200.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. São Paulo. Saraiva, 2009, p.250-251.

Tramitou na Câmara dos Deputados. Informação disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. Transformado na Lei Ordinária 12.965/2014.

De acordo com a Internet World Stats, site que contém uma grande quantidade de estatísticas atualizadas sobre a internet e a sua utilização em diferentes países, em junho de 2014, 3,03 bilhões de pessoas são usuárias da internet, o que representa 42,03% da população mundial. Informação disponível em: <http://www.internetworldstats.com/stats.htm>. Acesso em: 8 mar. 2020.

[...] com a implementação em andamento do IPv6, a versão ampliada e aprimorada dos endereços de protocolo de internet, haverá desenvolvimento do que é chamado “Internet das Coisas”, também conhecida pela sigla “IoT”, no termo em inglês. Praticamente qualquer dispositivo poderá estar conectado à internet e terá um endereço próprio.

Nesse contexto, é ressaltado ainda que, remotamente, poder-se-á visualizar informações do sistema de segurança da própria casa, bem como consultar a geladeira, podendo ter ou não determinado alimento. Outro recurso tecnológico é a instalação de um sensor infravermelho na entrada de um estabelecimento para ser feita a contagem de pessoas que adentram o ambiente e transmissão em tempo real das informações para a internet. Os próprios dispositivos interconectados pela internet poderão trocar informações entre si. As possibilidades são infindáveis. A princípio parece ficção científica, mas é realidade<sup>149</sup> ainda pouco perceptível pelas pessoas e muito superficialmente pelo cenário político e jurídico.

A compreensão dos interesses subjacentes de toda essa superestrutura em teia demanda uma visão sistêmica<sup>150</sup>, tendo em vista que a dinâmica dessa estrutura funciona em rede. Se assim não for observada, tornar-se-ão imperceptíveis tais interesses, bem como as soluções jurídicas já feitas e as que necessitam ser construídas, para atender ao direito fundamental à proteção dos dados pessoais, serão inúteis. Em termos jurídicos significa garantir o acesso mais amplo possível a todas as informações socialmente relevantes, públicas e privadas, por meio de uma nova geração de leis sobre o acesso às informações, mediante os mais diversos recursos tecnológicos; impedir que as coletas de dados pessoais se transformem em instrumentos de discriminação ou retaliação política; e reagir a qualquer forma de transformação da pessoa humana em número ou mercadoria<sup>151</sup>. Por isso, Castells é categórico em afirmar que “para fazer valer seus interesses, o comércio e os governos ameaçam conjuntamente a liberdade ao violar a privacidade em nome da

<sup>149</sup> Vale lembrar que o comunicador interestrelar no filme Jornada nas Estrelas produzido na década de 1960, hoje é o telefone celular.

<sup>150</sup> Nessa visão, amplia-se o foco de observação para se poder ver os sistemas dos sistemas, contextualizar o fenômeno e focalizar as interações recursivas (complexidade); admite-se a incontornabilidade do processo de mudança (instabilidade); acata-se outras descrições e atua na perspectiva de co-construção das soluções (intersubjetividade). VASCONCELLOS, Maria José Esteves de. Pensamento sistêmico: o novo paradigma da ciência. São Paulo: Papirus, 2008. p. 147-154.

<sup>151</sup> RODOTÁ, Stefano. **A Vida na Sociedade da Vigilância: A Privacidade Hoje**. São Paulo: Renovar, 2008, p. 161.

segurança”<sup>152</sup>.

Importante destacar nessa quadra o fato que foi considerado um escândalo como uma grave violação de dados pessoais sem o conhecimento e consentimento de seus titulares, quando um ex-diretor de Tecnologia de uma companhia com sede em Londres declarou que tal empresa de tecnologia comprou dados de milhões de usuários de uma rede social sem o consentimento dos usuários<sup>153</sup>. Segundo o que foi noticiado em todo o mundo, os dados foram obtidos por meio de um aplicativo de perfil psicológico desenvolvido por um pesquisador da Universidade Cambridge, o qual permitia ter acesso a informações não apenas de quem utilizava a rede social, mas também de seus amigos identificados pela ferramenta tecnológica. Tal fato fez com que a empresa de tecnologia deixasse de operar e pedir falência.

Cabe mais uma vez ressaltar que a principal questão não é rechaçar a introdução das tecnologias da informação nos mais diversos setores das atividades do setor público ou privado, as quais estão proporcionando uma gestão de informações que favorecem uma maior eficiência de seus serviços.

A questão é como compatibilizar esse avanço tecnológico com a proteção dos dados pessoais e, por consequência, tutelando alguns dos direitos da personalidade. Assim, a relevância está em que todas essas atividades devem ser pautadas nas necessidades primordiais do ser humano, se protegendo todos os direitos relacionados com a privacidade e possibilitando o desenvolvimento enquanto pessoa, da qual a dignidade lhe é inerente.

---

<sup>152</sup> CASTELLS, Manuel. **A Galáxia Internet**: reflexões sobre a internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p.150.

<sup>153</sup> Caso Cambridge Analytica e Facebook em 2018 – Segundo o Facebook, não foram 45 milhões, mas 87 milhões as contas afetadas pelo vazamento de dados da Cambridge Analytica, sendo 81,6% delas (70.632.350) de norte-americanos [...] No Brasil, o número de afetados foi de 443.117, segundo anunciou o diretor de tecnologia da empresa, Mike Schroepfer. Fonte: El País. Informação disponível em: [https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235\\_618558.html?rel=mas](https://brasil.elpais.com/brasil/2018/04/04/tecnologia/1522874235_618558.html?rel=mas). Acesso em: 8 mar. 2020.



## **CAPÍTULO 3**

### **PROTEÇÃO DE DADOS *VERSUS* TECNOLOGIA DA INFORMAÇÃO**

Este capítulo dedica-se a contrapor a proteção de dados ao desenvolvimento tecnológico. Neste contexto, explica os direitos centrais relacionados à proteção de dados e à privacidade; expõe o tratamento dado aos dados pessoais; e no confronto entre inteligência artificial e proteção de dados, busca encontrar caminhos para conciliar estas duas realidades tendo em vista que não se mostra razoável limitar excessivamente a divulgação de dados pessoais e nem permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação.

#### **3.1 DIREITOS CENTRAIS RELACIONADOS À PROTEÇÃO DE DADOS E À PRIVACIDADE**

Muitos direitos se relacionam à proteção de dados, sendo os citados com maior frequência na literatura, o direito à informação, o direito à intimidade e o direito à privacidade. Nesta seção dar-se-á ênfase aos dois últimos: intimidade e privacidade.

##### **3.1.1 Direito à Intimidade e à Privacidade**

Preliminarmente, uma questão que dificulta o entendimento da privacidade consiste no fato de que o instituto envolve diversos aspectos, ou dispõe de vários âmbitos de proteção: “honra”, “imagem”, “intimidade”, “vida privada”<sup>154</sup>. Tal consideração demonstra que o consenso conceitual pelos doutrinadores também em relação à privacidade é extremamente difícil. Devido a essa complexidade, quando ocorre violação de um direito, nem sempre ocorre, necessariamente, a violação dos demais.

Com isso, a dificuldade em conceituar “privacidade” e “intimidade” advém da própria extensão e do próprio conteúdo desses direitos. Normalmente, é

---

<sup>154</sup> GAMIZ, Mario Sergio de Freitas. **Privacidade e Intimidade**. Curitiba: Juruá Editora, 2012, p. 41.

apresentada por meio de interesses caracterizados por objetivos diversos. Nesse aspecto, a privacidade tem por objetivo proteger o homem contra: 1. Uma diversidade de invasões que possam influenciar em sua vida particular, familiar e doméstica; 2. A comunicação de acontecimentos importantes e embaraçosos afetos à sua intimidade; e 3. A transmissão de informações enviadas ou recebidas decorrente de segredo profissional. Entretanto, existem inúmeros obstáculos para a referida conceituação, conforme retrata Silva:

São inúmeras as dificuldades que o tema suscita. A primeira delas é precisar a extensão e o conteúdo desse direito, cujo interesse subjacente é de caráter eminentemente subjetivo, por isso mesmo variável de pessoa para pessoa; os valores sociais são diferentes e mutáveis no tempo e no espaço; o sentimento que constitui o seu núcleo oscila no âmbito de cada pessoa. Essa dificuldade ainda mais se evidencia nas tentativas dos autores em formular uma definição do direito à intimidade. Torna-se mais difícil ainda quando se tem que estabelecer em que medida ou em que situações o interesse de preservação da intimidade deve ser sacrificado em prol de um outro interesse juridicamente protegido, quando os dois se colocam em posição de absoluto antagonismo<sup>155</sup>.

Fora esses aspectos, um ponto que contribui para dificultar o consenso no entendimento da questão provém do fato de que diplomas legais ou convenções internacionais tendem a não cuidar de precisar seu conceito. Exemplo disso é visto na CRFB/1988 brasileira, que identifica as situações pelas quais o referido direito não pode ser violado, todavia, em nenhum momento, estabelece qualquer noção conceitual sobre o tema. Diante disso, os doutrinadores não possuem uma base inicial que possa servir de referência.

Além desses fatores, outra questão que torna essa tarefa árdua advém do pluralismo social: os valores entre as diferentes comunidades não são homogêneos ou iguais. Em adição às condições sociais, os aspectos materiais afetam significativamente o entendimento do direito à intimidade.

Para Sarlet, Marinoni e Mitidiero<sup>156</sup>, por exemplo, a densidade da população, o grau de interação, as condições de residência, a divisão do trabalho, a

---

<sup>155</sup> SILVA, Edson Ferreira da. **Direito à intimidade**: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002. São Paulo: Juarez Soares, 2003, p.4-5.

<sup>156</sup> SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2014, p.115.

natureza da família e outras relações sociais devem ser considerados como fatores determinantes na definição do referido direito.

Nessa mesma linha de pensamento, Doneda<sup>157</sup> destaca que a definição de privacidade não é um problema puramente dogmático, visto que se encontra estreitamente relacionada aos valores e projeções humanas em cada sociedade e, no âmbito de cada um dos muitos grupos, esta tarefa possui forte conteúdo social e também ideológico. Desta forma, há uma multiplicidade de opiniões arroladas acerca do tema.

Há, ainda, necessidade de buscar um mínimo de conteúdo – apto a satisfazer as garantias pessoais dos cidadãos das sociedades – que seja comum para o entendimento do direito à privacidade. Todavia, Leal<sup>158</sup> pontua que não se pode, a princípio, definir, em toda a sua plenitude, a intimidade e a vida privada posto que seus contornos inequívocos só podem ser mensurados, considerando suas especificidades e o contexto em que ocorreu o caso concreto.

A situação em pauta conduz à noção de que a privacidade é um problema que o meio jurídico necessita solucionar, principalmente agora, com o avanço tecnológico e, em especial, com a proliferação do acesso à internet.

É importante também distinguir privacidade de direito à privacidade. Sobre essa dicotomia, nas várias consultas bibliográficas realizadas na doutrina brasileira, não se vislumbrou – de forma clara e objetiva – a preocupação dos estudiosos pátrios com o tema. Entretanto, na doutrina norte-americana, Solove, Rotenberg e Schwartz<sup>159</sup>, por meio de sua obra *Privacy Information and Technology*, tratam do assunto como preliminar para a defesa do entendimento do referido direito numa visão pragmática. Nesse sentido, o direito da privacidade diz respeito às medidas pelas quais ela deve ser legalmente protegida. Então, por essa linha de raciocínio, entende-se como tal, no Direito brasileiro, o constante dos incs. X, XI e

---

<sup>157</sup> DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p.139.

<sup>158</sup> LEAL, Luziane de Figueiredo Simão. **Crimes Contra os Direitos da Personalidade na Internet**. Curitiba: Juruá Editora, 2015, p.123.

<sup>159</sup> Apud SOLOVE, Daniel J; ROTENBERG, Marc; SCHWARTZ, Paul M. **Privacy, information, and technology**. New York: Aspen Publishers, 2006, p.129.

XII do art. 5º da CRFB/1988. Em contrapartida, “privacidade” abarca todo o conceito que não esteja inserido em documento legal, vislumbrado, por conseguinte, como um valor a ser compreendido.

Contribui, outrossim, para a complexidade do entendimento da privacidade – dificultando a elaboração de um conceito fechado sobre o tema – a possibilidade de renúncia, ainda que temporária, do direito à privacidade, o que decorre do fato de ele mesmo integrar o direito da personalidade e apresentar a característica, entre outras, de não ser absoluto.

No espaço virtual, isso ocorre normalmente quando um indivíduo se associa a uma rede social na Internet – trata-se de uma teia de conexão de um grupo de pessoas que se comunicam entre si, podendo ou não ter uma relação estreita de amizade. Nesse contexto, as pessoas costumam preencher perfis em que normalmente constam números de telefone, endereço de e-mail e outros dados pessoais que podem estar disponíveis apenas a um grupo fechado de indivíduos ou ser totalmente acessíveis ao público em geral.

Nesse novo contexto, quando o internauta disponibiliza informações *on-line*, ele não está apenas renunciando à sua privacidade: muitas vezes, restringe igualmente a privacidade de seus pais, de amigos e de outras pessoas sem que eles tenham sequer conhecimento disso. O problema, então, é que muitas informações disponibilizadas na Internet são preservadas para sempre – até pelo fato de alguém copiá-las e mantê-las a seu bel-prazer na rede.

Canotilho e Machado<sup>160</sup>, em estudo sobre a privacidade contemporânea, destacam que as expressões “intimidade” e “vida privada” carecem de interpretações consoante o contexto variável e possível de mudanças no tempo e no espaço. Assim sendo, o conceito de privacidade poderá adquirir maior ou menor elasticidade, dependendo da evolução da mentalidade da época, da identidade dos indivíduos envolvidos, de sua função social e estilo de vida dos interessados. Assim, quando uma pessoa decide tornar público seu comportamento (geralmente

---

<sup>160</sup> CANOTILHO, J.J. Gomes; MACHADO, Jónatas E.M. **“Reality Shows” e Liberdade de Programação**. Coimbra: Coimbra Editora, 2003, p.52-53.

protegido pelo direito à privacidade), ela não renuncia totalmente ao referido direito, apenas passa a exercê-lo conforme suas preferências. Assim, a privacidade não pode ser analisada de forma generalizada e única para todos: necessita avaliação conforme o caso concreto.

### 3.1.2 Direito à autodeterminação informativa

A primeira lei sobre a proteção de dados pessoais foi na Alemanha, a lei do Land de Hesse, de 1970. Segundo Doneda<sup>161</sup> a República Federal da Alemanha possuía, desde 1977, uma lei federal de proteção de dados pessoais, a *Bundesdatenschutzgesetz*. Os trabalhos do censo alemão, os quais foram regulamentados por uma lei aprovada em 1982, deveriam ser finalizados em 1983. Entretanto, provocaram desconfiança em vários setores da sociedade, quanto ao método de coleta de informações utilizado e pela destinação destas. Esta foi a causa de uma célebre sentença da Corte Constitucional Alemã (*Bundesverfassungsricht*), a qual até hoje é referência no tema da proteção de dados pessoais.

Tal lei que organizava o censo foi a causa da sentença. Previa, segundo Mèlo<sup>162</sup> que cada cidadão deveria responder a 160 perguntas, as quais seriam posteriormente submetidas a tratamento informatizado. Permitia-se também que os dados recolhidos no censo fossem rastreados até os cidadãos recenseados e fossem utilizados para outras finalidades diversas do recenseamento, como, e.g., pelas autoridades locais para corrigir os cadastros de moradores dos municípios.

A decisão proferida pelo Tribunal Constitucional Federal Alemão em 25.12.1983 concordou com os propósitos estatísticos da lei, porém declarou que os direitos fundamentais dos cidadãos deveriam ser protegidos contra certos abusos. Entendeu que a transferência de dados obtidos no recenseamento do governo federal para autoridades locais seria inconstitucional.

---

<sup>161</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.192.

<sup>162</sup> MÊLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019, p. 119.

Apesar de tal situação na decisão dizer respeito ao princípio da finalidade, a doutrina é uníssona em afirmar que nessa decisão foi reconhecido o direito à autodeterminação informativa.

Segundo Ruaro<sup>163</sup>, a autodeterminação informativa é a possibilidade de um indivíduo, titular de determinado dado, exigir que seus dados não sejam tratados. Dito de outra forma é a capacidade, possibilidade e liberdade que as pessoas têm para decidir sobre o tratamento de seus dados, e se desejarem, interromper este tratamento.

Conforme acentua Rodotà<sup>164</sup> esse direito considera ilegítima toda coleta de informações pessoais que for realizada sem um prévio conhecimento e explícito consentimento do interessado. Esse direito consiste em que determinadas informações coletadas sobre uma determinada pessoa não devem circular fora da instituição pública ou privada que tenha coletado essas informações originalmente para certa finalidade.

Segundo a previsão da Lei 12.965/2014<sup>165</sup>, tal direito encontra plasmado nos dispositivos que: 1) veda o fornecimento a terceiros de registros de conexão e de acesso à aplicações de Internet, exceto mediante consentimento livre, expresso e informado; 2) exige clareza e completude das informações sobre a coleta, uso, tratamento e proteção de seus dados pessoais; e 3) que somente poderão ser utilizados para as finalidades que fundamentaram sua coleta.

A Lei 13.709/2018 prevê expressamente que a autodeterminação informativa é um dos fundamentos da disciplina da proteção de dados pessoais<sup>166</sup>. A resultante dessa previsão está no elenco de direitos previstos, os quais são: a) à confirmação da existência de tratamento; b) ao acesso aos dados; c) à correção de dados incompletos, inexatos ou desatualizados; d) à anonimização<sup>167</sup>, bloqueio ou

---

<sup>163</sup> RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina – PI, v.2, n.1, p.41-60, Jan./Jun., 2015, p.43.

<sup>164</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.75.

<sup>165</sup> Incs. VI e VII do art. 7º da Lei 12.965/2014.

<sup>166</sup> Art. 2º da Lei geral de proteção de dados pessoais.

<sup>167</sup> Termo novo na legislação pátria cujo conceito previsto na Lei é a utilização de meios técnicos

eliminação de dados desnecessários, excessivos ou tratados desconformes com as disposições legais; e) à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e desde que observados os segredos comercial e industrial, conforme a regulamentação do órgão controlador; f) à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses de conservação dos dados previstas na Lei<sup>168</sup>; g) à informação das entidades públicas e privadas com as quais o controlador compartilhou dados; h) à informação acerca da possibilidade de não conceder consentimento e sobre as consequências da negativa; e i) à revogação do consentimento.

Vê-se que a finalidade legal é atribuir à pessoa, o direito de saber o que é feito com as informações pessoais e decidir se autoriza ou não a utilização para fim diverso da que foi obtida.

Porém, surge uma questão essencial: como esse controle pode ser exercido pela pessoa para assegurar esse direito? A resposta fundamental é que a questão passa a não ser mais jurídica. É questão de gestão de políticas públicas da qual o direito já regulou. Assim, no mesmo sentido que a engenharia informática é capaz de criar inteligências artificiais para tratar informações, por meio de métodos de análise os mais diversos, a criação de ferramentas para que o indivíduo possa ter esse conhecimento e manifeste seu consentimento é algo muito simples de ser desenvolvido e posto à disposição da pessoa que for alvo dessa situação. Eis mais um desafio para que tal direito possa ter efetividade.

Nether<sup>169</sup> explica que historicamente, assim como os regimes absolutistas foram dando lugar a regimes democráticos, em diversos países no mundo, esse direito à autodeterminação informativa está sendo reconhecido gradativamente pelos sistemas jurídicos, e se consolidando como resultante da afirmação constante da

---

razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

<sup>168</sup> Art. 16. [...] autorizada a conservação para as seguintes finalidades: I – cumprimento de obrigação legal ou regulatória pelo controlador; II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei;

<sup>169</sup> NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018, p.59.

necessidade de regimes democráticos. Como se vê, no Brasil está em fase inicial ou embrionária, tendo em vista a fase que se encontra a recente vigência da Lei. Esse direito, como derivante do direito fundamental à proteção dos dados pessoais, está sendo imprescindível nos dias atuais.

Dito isto, é possível constatar que os dados pessoais devem ter um significado e valor diferentes, bem como mais abrangentes de quando foi incluso no rol de direitos fundamentais na década de 1980, quando da promulgação da Constituição da República Federativa.

### 3.2 OS DADOS PESSOAIS E SEUS TITULARES

A doutrina pátria basicamente classifica-os em dois tipos: sensíveis e não sensíveis. Monteiro<sup>170</sup> afirma que os dados pessoais sensíveis são os que estão substancialmente ligados à esfera de privacidade. Exemplifica a origem racial, a saúde física e mental, crenças religiosas, traços da personalidade, orientação sexual, registros policiais, dentre outros. Os não sensíveis são os que, em tese, pertencem ao domínio público, são suscetíveis de apropriação por qualquer pessoa e podem ser armazenados e utilizados sem causar danos. Exemplifica o nome, estado civil, domicílio, profissão, grupos associativos etc. Afirma-se que a difusão ou a utilização indevida de dados pessoais não sensíveis raramente causam violações à vida privada.

Ocorre que em virtude de vários fatores sociais atuais, cujo mais determinante é o avanço da tecnologia da informação, especialmente a utilização da Internet como meio de comunicação e obtenção de informações, por intermédio da “mineração de dados”<sup>171</sup>, a utilização de determinados dados considerados não sensíveis por terceiros, a exemplo do domicílio e profissão, sem o conhecimento do titular, em determinadas circunstâncias pode causar danos à pessoa. Nessas

---

<sup>170</sup> MONTEIRO, Carina Villela de Andrade. Direito à Privacidade versus Direito à Informação. **Revista de Informação Legislativa**, Brasília, a.44, n. 173, p.27-40, jan./mar. 2007, p.33.

<sup>171</sup> O processo de minerar dados visa descobrir conexões escondidas e prever tendências futuras (...) o termo “mineração” só foi cunhado nos anos 1990, mas sua base compreende três disciplinas científicas interligadas: a estatística (o estudo numérico das relações entre dados), a inteligência artificial (inteligência exibida por softwares e/ou máquinas, que se assemelha à humana) e a *machine learning* (algoritmos que podem aprender com dados para realizar previsões) (MÊLO, 2019, p. 116).



condições, o fator determinante é a intenção desses terceiros na utilização desses dados, sem que o indivíduo saiba qual o propósito dessa “mineração”.

Portanto, dados pessoais “são quaisquer informações relacionadas com a pessoa titular que, a depender da associação de um determinado dado com outro, forma um conjunto de informações que podem ser utilizadas para os mais diversos fins [...]”. A Lei 12.965/2014 traz algumas definições essenciais para esse cenário, porém, não prevê a definição do que sejam dados pessoais. A definição prevista na Lei de proteção de dados pessoais foi simplória, definiu como “informação relacionada a pessoa natural identificada ou identificável”<sup>172</sup>.

Nessa perspectiva, dados pessoais podem ser os mais diversos. Essa divisão dicotômica trabalhada na doutrina não atende à complexidade das circunstâncias atuais, e limita a análise de casos concretos, especialmente os mais complexos. Por isso, “mesmo dados não qualificados como sensíveis, quando submetidos a um determinado tratamento, podem revelar aspectos da personalidade de alguém, podendo levar a práticas discriminatórias”<sup>173</sup>.

Portanto, dados pessoais, da maneira como definida no sistema europeu, podem ser: uma imagem, uma conversa gravada, uma filmagem, hábitos de consumo pessoal, registrados por meio de Internet ou administradora de cartão de crédito, dentre outras informações. Vê-se que as possibilidades são várias, devido a tudo estar interligado tecnologicamente nos dias atuais, num maior ou menor grau. Assim, simples dados cadastrais se cruzados e tratados com outros de outro sistema, mediante a mineração de dados, podem detalhar quase muitos os aspectos da vida de uma pessoa.

Inúmeros acontecimentos podem ser encontrados que retratam como a informação tem sido veiculada nos mais diversos meios de comunicação, e as atividades realizadas no dia a dia em que a tecnologia da informação é algo

---

<sup>172</sup> BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). 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: 22 jan. 2020.

<sup>173</sup> DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006, p.162.

indispensável. Freire<sup>174</sup> elenca algumas das atividades do cotidiano das pessoas e cita que, basicamente, terceiros estranhos a todas as comunicações feitas individualmente, quando se utiliza qualquer recurso tecnológico, sabem minimamente, quem e o que se faz, quando e como está sendo feita, qual o conteúdo da comunicação, o quanto está se pagando quando é onerosa, onde a pessoa está ou para onde se dirige, e a frequência com que é feito o quê.

Todas essas possibilidades existem efetivamente e se concretizam em registros, quando se conecta à internet para: a) receber ou enviar e-mail, b) comprar produtos ou solicitar serviços, c) reservar e/ou comprar passagens, d) se cadastrar para obter informações em sites; também ocorre quando: acessa caixas eletrônicas, utiliza a rede de telefonia móvel, passa por estradas com pedágio ou quando vias públicas estão sendo filmadas, usa o cartão de crédito, dentre outras.

Sob a principal justificativa de questões de segurança, as sociedades em que os países possuem a tecnologia da informação a serviço da iniciativa privada, estão sendo constantemente monitoradas. Entretanto, o propósito não é somente a segurança, a prática demonstra outros. Matéria publicada no jornal Folha de S. Paulo<sup>175</sup> destaca: “Loja filma todas as reações de seus consumidores”. Noticiou-se que qualquer pessoa que esteja fazendo compras num shopping de Mineápolis, no Estado de Minnesota<sup>176</sup>, EUA, terá suas reações registradas por circuitos eletrônicos, quando à frente dos produtos e ofertas, para serem analisadas por psicólogos, publicitários e analistas de mercado. Nesse mesmo shopping, uma determinada loja de departamentos<sup>177</sup> também resolveu instalar centenas de câmeras de circuito interno de TV, porém com microfones ultrassensíveis para gravar as conversas sobre as reações dos prováveis consumidores, além das imagens e saber quanto tempo ficam parados diante de um produto, qual o cartaz de ofertas que foi mais observado, quais as reações diante dos preços. A matéria faz menção também à advertência mediante cartaz de que o local está sendo filmado

---

<sup>174</sup> FREIRE, Alexandre. **Inevitável Mundo Novo**: O Fim da Privacidade. São Paulo: Axis Mundi, 2006, p.95-97.

<sup>175</sup> LIMBERGER, Têmis. O Direito à Intimidade na Era da Informática. Porto Alegre: Livraria do Advogado, 2007. p. 59.

<sup>176</sup> As leis do referido Estado permitem que os proprietários filmem e gravem seus clientes, desde que não nos provadores.

<sup>177</sup> *Once Famous*.

para testes, e com o aviso de que se a pessoa se sentir incomodada com situação que retorne em outro momento.

Esse fato provavelmente se repete em muitos outros lugares deixando a sensação de insegurança.

Destaca Freire<sup>178</sup> que um detetive da Web<sup>179</sup> foi desafiado para que, com a utilização do nome completo, descobrisse o máximo possível de informações sobre a pessoa que o desafiava, utilizando a internet. Em dois dias ele retornou com um telefonema informando a data do nascimento, o endereço de residência e o número do CPF. Informou que apesar de retornado com dois dias, obteve essas informações em cinco minutos. Prometeu que em cinco dias teria mais informações pessoais. E para surpresa da desafiante, desmoronou qualquer noção de privacidade que se tinha. Com um computador e acesso à internet e um telefone, conseguiu informações sobre detalhes mais reservados da vida privada como, para quem telefona tarde da noite; quanto tem disponível em dinheiro no banco; quanto recebe; quanto paga de aluguel; dois números de telefones que não constam na lista. Esse caso foi publicado na revista Forbes<sup>180</sup>, e o autor alerta que a perda da privacidade é muito maior do que se imagina, porque os avanços nas técnicas de pesquisa inteligente de dados e a formação de base de dados estratosféricas demonstram que a expansão da rede é a etapa final, no sentido de que os sistemas deixarão todos os seus segredos disponíveis para serem revelados sem seu consentimento com uns poucos toques de teclados.

Adverte ainda o autor<sup>181</sup> que um grande banco brasileiro está desenvolvendo um projeto no qual quando um cliente com determinado perfil chegar à agência bancária para fazer qualquer operação, o seu gerente saberá da sua chegada ao banco por meio de uma mensagem que aparecerá na tela do seu computador. Esse monitoramento será feito com base em qualquer dado do cliente reconhecido pelos instrumentos tecnológicos instalados no banco, o qual pode ser

---

<sup>178</sup> FREIRE, Alexandre. **Inevitável Mundo Novo: O Fim da Privacidade**. São Paulo: Axis Mundi, 2006, p.135-136.

<sup>179</sup> Dan Cohn e sua agência privada de detetives da internet, a Docusearch.

<sup>180</sup> Texto original disponível em: <http://www.forbes.com/forbes/1999/1129/6413182a.htm> e <http://penenberg.com/story-archive/the-end-of-privacy/>. Acesso em: 17 mar. 2020.

<sup>181</sup> FREIRE, Alexandre. **Inevitável Mundo Novo: O Fim da Privacidade**. Op. cit. p. 136.

desde uma câmera de segurança na entrada da agência, até um terminal utilizado pelo cliente. Por meio desse sistema seu gerente receberá, instantaneamente, todas as informações bancárias necessárias, e saberá qual produto mais adequado poderá lhe oferecer. Afirma-se que esse projeto é de “relacionamento com o cliente”. Porém, cabe o seguinte questionamento: este tipo de relacionamento em que alguém está sendo vigiado sem saber seria um relacionamento transparente? Inexiste dúvida que transparente fica o indivíduo que é objeto de interesse do banco, porém sua estratégia nada tem de transparente. Outro fato também é citado<sup>182</sup>: inúmeros sites de busca especializados estão se expandindo na internet, sem qualquer controle. Mediante a cobrança de determinados valores, é prestado um serviço de fornecimento de informações pessoais, a exemplo do nome e endereço completo, histórico de endereços anteriores com os respectivos números de telefones, ações que tramitaram ou em andamento no Judiciário, os bens que possui e todas as características peculiares, tudo isso sem que o titular dessas informações saiba que está sendo pesquisado<sup>183</sup>.

Por isso cita também que os limites da vida privada, independentemente da classe social, nacionalidade, credo, cor ou opção sexual, diminuem a cada dia de maneira imperceptível com a popularização dos diversos aparelhos eletrônicos (telefones celulares, câmeras fotográficas e de vigilância, computadores, palmtops, *notebooks*). Sem perceber, as pessoas estão substituindo sua privacidade pelas informações e facilidades que a tecnologia oferece, principalmente para atender os interesses de empresas que querem saber suas preferências e hábitos de consumo<sup>184</sup>.

Parece que todas essas situações previstas em ficção, mais cedo ou mais tarde estão ocorrendo no dia a dia das pessoas, mesmo no daquelas que não disponham de recursos tecnológicos enquanto consumidor de produtos, mas pelo simples fato de ser uma pessoa no mundo.

---

<sup>182</sup> FREIRE, Alexandre. **Inevitável Mundo Novo**: O Fim da Privacidade. São Paulo: Axis Mundi, 2006, p.139.

<sup>183</sup> Podem ser destacados os sites: NomesBrasil.com. Disponível em: <http://www.nomesbrasil.com.br/> e todosobretodos, disponível em: <http://tudosobretodos.se/>. Este oferece planos de acessos aos demais dados como CPF, endereço completo, parentes, empresas e sociedades, endereços alternativos e “prováveis redes sociais”.

<sup>184</sup> FREIRE, Alexandre. **Inevitável Mundo Novo**: O Fim da Privacidade. Op. cit.

Segundo Rodotà<sup>185</sup>, o problema da privacidade das informações apareceu somente em relação aos dados relacionados à atividade econômica, nos seis primeiros censos feitos nos Estados Unidos entre 1790 e 1840. Era uma consequência óbvia da estrutura dos sistemas jurídicos burgueses, nos quais os direitos da personalidade eram formalmente reconhecidos principalmente na perspectiva da garantia da propriedade. O privilégio reservado às informações econômicas, sob o perfil do sigilo, constituía-se em um instrumento que reforçava a posição de proprietários e empreendedores, portanto, livres de controles contínuos e substanciais por parte da coletividade.

As circunstâncias nas quais a privacidade é concebida nos dias atuais demanda uma análise diferente da que era feita nos séculos passados e antes do advento das tecnologias da informação, principalmente quando as políticas atuais de mercado de consumo de produtos, que favorecem a informação e a comunicação estão cada dia buscando abranger um número cada vez maior de pessoas.

Diante dessas circunstâncias sociais, mercadológicas e tecnológicas, dados pessoais que necessitam de proteção jurídica, podem ser os mais diversos. Nesse cenário de avanço tecnológico, pode ser uma imagem, uma conversa, uma filmagem, hábitos de consumo pessoal, registrados por meio de operações via internet ou administradoras de cartões de crédito, dentre outras informações. Vê-se que as possibilidades são as mais variadas, principalmente devido tudo estar interconectado ou em vias de se estar.

Diante desse panorama, a Lei 13.709/2018 deveria prever uma definição mais ampla possível do que seriam dados pessoais, como ocorre na legislação interna dos países europeus que legislaram primeiramente sobre a matéria, tendo em vista o caráter geral da Lei geral de proteção de dados pessoais<sup>186</sup>. Outra razão para se trazer essa definição mais ampla é que o Brasil faz parte da Rede Ibero-americana de Proteção de Dados – RIPD e o interesse primordial das instituições

---

<sup>185</sup> RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p.34.

<sup>186</sup> NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018, p.140.

que atualmente constituem esta Rede é continuar promovendo o desenvolvimento do direito fundamental à proteção de dados pessoais, a fim de conseguir obter adequação ao sistema europeu de proteção desses dados.

O Brasil, trilhou paulatinamente este caminho e a LGPD muito se assemelha à *General Data Protection Regulation*, conforme se viu no primeiro capítulo.

A LGPD foi construída com base na RGD. Ela também tem jurisdição global, pois qualquer site, sediado em qualquer nação que atue processando dados pessoais de cidadãos brasileiros precisa cumpri-la.

Quanto aos fundamentos legais referentes ao processamento de dados, Castro<sup>187</sup> demonstra que a LGPD difere somente superficialmente da RGD quando se trata de sua base legal direcionada ao processamento de dados. Assim, a LGPD e a RGD se encontram alinhadas, com pequenas variações. No ponto em que a RGD conta com 6 bases legais para processamento, identifica-se 10 na LGPD. Esta última divide a redação mais geral do RGD em disposições mais específicas.

A título de exemplificação, o fundamento legal da RGD cujo preceito é “salvar a vida de alguém”, na LGPD apresenta a seguinte divisão: “a) proteger a vida ou a segurança física; e, b) proteger a saúde, em um procedimento realizado por profissionais de saúde ou por entidades de saúde”<sup>188</sup>.

Ademais, a LGPD apresenta como *plus* uma fundamentação legal referente à proteção do crédito que a RGD não adotou em sua completude.

Também, os dados pessoais têm uma definição mais ampla na LGPD do que na RGD. Segundo a LGPD, pode ser considerado como “dados pessoais” qualquer coisa que se relacione a uma pessoa singular possível de ser

---

<sup>187</sup> CASTRO, Nuno Teixeira. Um novo quadro legal europeu em matéria de proteção de dados vislumbrando o Mercado Único Digital para a Europa. **Diário Insonias**. [S.l.], 11.05.2016. Disponível em: <http://www.insonias.pt/um-novo-quadro-legal-europeu-materia-proteccao-dados-vislumbrando-mercado-unico-digital-europa/amp/>. Acesso em: 20 mar. 2020.

<sup>188</sup> BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). 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: 22 mar. 2020.

identificada. Na RGD, a especificação vem através de exemplos como nomes, gênero e endereços.

Castro<sup>189</sup> pontua que na LGPD, os dados sensíveis são, como na RGD, uma categoria distinta dos dados pessoais, incluindo informações sobre raça, etnia, crenças religiosas, ideias políticas, saúde, biometria, sexualidade, dentre outros. As limitações para que dados confidenciais sejam processados na LGPD são mais severas do que na RGD.

Outro ponto que observado por Lemoalle e Carboni<sup>190</sup> é que a LGPD não disponibiliza definições acerca dos dados pseudonimizados, assim como a RGD. A exceção são as pesquisas desenvolvidas por organizações que atuam na saúde pública. A seu turno, a RGD é bastante específica no que tange a seus requisitos referentes ao processamento de dados pessoais com fins de publicidade/marketing, enquanto a LGPD nada dispõe sobre o tema.

Importa destacar também que na RGD, foi instituída a Avaliação de Impacto na Proteção de Dados (AIPD) cujo objetivo é mensurar os riscos afetos ao processamento de dados. Também exige que os processadores notifiquem as autoridades responsáveis pela proteção de dados se forem identificados elevados riscos referentes ao processamento de dados.

Também, segundo Mèlo<sup>191</sup> a LGPD institui a AIPD, mas não deixa claro como esta avaliação deve ser empregada, nem disponibiliza requisitos para que quaisquer autoridades de supervisão sejam notificadas. No entanto, na LGPD é obrigatório para as empresas que contem com um oficial de proteção de dados (OPD), enquanto este profissional só é necessário em algumas poucas circunstâncias na RGD.

---

<sup>189</sup> CASTRO, Nuno Teixeira. Um novo quadro legal europeu em matéria de proteção de dados vislumbrando o Mercado Único Digital para a Europa. **Diário Insonias**. [S.l.], 11.05.2016. Disponível em: <http://www.insonias.pt/um-novo-quadro-legal-europeu-materia-proteccao-dados-vislumbrando-mercado-unico-digital-europa/amp/>. Acesso em: 20 mar. 2020.

<sup>190</sup> LEMOALLE, Edouard; CARBONI, Guilherme. **Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil**. JOTA. [S.l.], 12.02.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018>. Acesso em: 20 mar. 2020.

<sup>191</sup> MÈLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019, p. 123.

As restrições de tempo para que as violações de dados sejam notificadas são especificadas explicitamente na RGPD (72 h), enquanto a LGPD ordena livremente que as violações sejam notificadas às autoridades em “tempo razoável”<sup>192</sup>.

Referente às multas, Lemoalle e Carboni<sup>193</sup> destacam que, comparada com a RGPD, na LGPD, caso ocorram violações por não conformidade, as penalidades são menos severas. Os valores máximos das multas por não conformidade na RGPD encontram-se fixados em 20 milhões de euros o que corresponde a 4% do faturamento anual global de uma organização. A LGPD limita suas multas a um máximo de 50 milhões de reais (aproximadamente 11 milhões de euros) ou 2% do que uma empresa fatura anualmente no Brasil.

Quanto às aplicações territoriais, a LGPD trata a transferência de dados pessoais em âmbito internacional da mesma forma que a RGPD, avaliando se no outro país vigoram leis adequadas para a proteção de dados. No entanto, a LGPD (ao contrário da RGPD) não determina que os dados devem ser transmitidos pelo Brasil sem nenhum processamento adicional.

### 3.3 O CONFRONTO: INTELIGÊNCIA ARTIFICIAL E A PROTEÇÃO DE DADOS

Frente à evolução tecnológica e, conseqüentemente, maior recorrência de violação à privacidade, necessário se faz conjunto de normas que possam disciplinar a responsabilidade e a transparência na era digital. Normas que não obstem a inovação e o desenvolvimento tecnológico, mas que acompanhem a revolução tecnológica de forma que as vantagens da IA sejam amplamente empregadas, evitando na medida do possível seus perigos potenciais<sup>194</sup>.

Antes de contrapor a inteligência artificial à proteção de dados, é

---

<sup>192</sup> MÊLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019, p. 123.

<sup>193</sup> LEMOALLE, Edouard; CARBONI, Guilherme. **Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil**. JOTA. [S.l.], 12.02.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018>. Acesso em: 20 mar. 2020.

<sup>194</sup> SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. *Unio – EU Law Journal*, v.4, n.2, p.1-17, 2018, p.6.



importante discutir um conceito de grande relevância, qual seja, o de internet das coisas (*Internet of Things* – IoT).

A IoT pode ser vista como a rede global com a funcionalidade de integrar o mundo físico. Isso se dá por meio da coleta, do processamento e da análise de dados gerados pelos sensores da IoT, que estarão presentes em todas as coisas e se integram por meio da rede mundial. “Importante anotar que a Internet das Coisas apenas é possível em razão do advento do modelo IPV6, sem o qual não haveria tantos números de protocolos disponíveis para conectar essa infinidade de aparelhos”<sup>195</sup>. Esse modelo IPV6, em resumo, é uma nova versão do chamado “protocolo IP”, o qual surgiu em 1993 e permitiu um crescimento mais ordenado da rede, eliminando restrições dos protocolos anteriores. O Comitê Gestor da Internet no Brasil conta que, com um maior crescimento da rede, em dezembro de 1993 a IETF (*Internet Engineering Task Force*, grupo informal internacional composto de técnicos, agências, pesquisadores, que, em conjunto com outros órgãos, trabalha para o desenvolvimento e promoção de padrões para Internet) – formalizou as pesquisas a respeito de um novel padrão do protocolo IP, definindo e estabelecendo uma nova e melhorada versão chamada de IPV6<sup>196</sup>.

Entre outras coisas, a IoT pode prever a manutenção e a demanda de equipamentos, facilitando os produtores a cobrarem o equipamento não mais tanto na sua aquisição, mas sim mais de fato pelo seu uso – o chamado *power by the hour*.

No geral, as empresas que criam e se apropriam da tecnologia da IoT, incluindo aqui dispositivos que fazem uso da inteligência artificial, dizem que, com maior disponibilidade de dados, há enormes oportunidades para melhor tomada de decisões e desenvolvimento de estratégias, apresentando tecnologias inovadoras para a próxima geração.

---

<sup>195</sup> FLORENCIO, Juliana Abrusio. **Proteção de dados na cultura do algoritmo**. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019, p.77-78.

<sup>196</sup> COMITÊ GESTOR DA INTERNET NO BRASIL. **A internet e o TCP IP. IPV6**. 15 mai. 2012. Disponível em: <http://ipv6.br/post/introducao/>. Acesso em: 12 mar. 2020.

Por outro lado, Benjamin Cabé, gerenciador de programação de IoT para a *Open Source Community*, esclareceu para o *IoT Developer Survey 2018* que tais inovações têm muitas vezes um lado sombrio, que envolve a aquisição, negociação e controle de informações, em suas palavras: “Eles não estão construindo um objeto conectado somente por construir um objeto conectado. É para colher os dados”<sup>197</sup>. Essa é a outra face da IoT, no que diz respeito a gerar “uma infinidade de dados (*big data*) e trazendo ainda mais desafios à proteção da privacidade e dos dados pessoais”<sup>198</sup>.

Os desafios jurídicos nesse setor são enormes e complexos, demandando novas maneiras de se pensar e construir enunciados capazes de proteger a privacidade das pessoas e seus dados. Assim, o que já se discute a partir da internet, adquire dimensões muito maiores em escala global e sistêmica.

Diversas organizações estão começando a transmitir os dados coletados pela IoT para terceiros. Muitas vezes isso é motivado pelo desejo de monetizar os dados. Essas iniciativas estão trazendo para o primeiro plano as questões de propriedade de dados, de privacidade e de licenciamento.

Não há ainda esquema definido para determinar, nesses casos envolvendo IoT, como a propriedade é atribuída, muito menos como os dados da IoT podem ser licenciados corretamente.

Essencialmente, o proprietário dos chamados *machine-generated data* (MGD), o que abrange praticamente toda a IoT, é a organização que detém o título do dispositivo que registrou os dados. Em outras palavras, a entidade proprietária do dispositivo IoT também possui os dados produzidos por esse dispositivo.

Além disso, como se sabe, os dados podem pertencer a uma parte e serem controlados por outra. A posse de dados não significa necessariamente o

---

<sup>197</sup> CABÉ, Benjamin. **Key trends from the IoT Developer Survey 2018**. Blog Benjamin Cabé. 17 abr. 2018. Disponível em: <https://blog.benjamin-cabe.com/2018/04/17/key-trends-iot-developer-survey-2018>. Acesso em: 22 mar. 2020.

<sup>198</sup> FLORÊNCIO, Juliana Abrusio. **Proteção de dados na cultura do algoritmo**. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019, p.78.

título. Posse é controle. Título é propriedade. Referidos como direitos de uso, cada vez que os conjuntos de dados são copiados, recopiados e transmitidos, o controle dos dados os acompanha<sup>199</sup>.

Ademais, enfrenta-se também o grande perigo de vazamento de dados. Por exemplo, em 2018, foi descoberto que o alto-falante doméstico de inteligência artificial do Google e o *Chromecast* revelam a localização física precisa de um usuário. Descoberto pelo pesquisador de segurança Craig Young, o *bug* pode tornar a localização de uma pessoa conhecida com uma precisão de cerca de 10 metros.

Apthorpe, Reisman e Feamster, do departamento de ciência da computação da Universidade de Princeton, avisou na época que “o problema real com esse vazamento de dados é que as redes domésticas não podem mais ser consideradas ambientes confiáveis”<sup>200</sup>. Além disso, ele explica que esse vazamento também indica como a IoT exige o endurecimento de ambientes confiáveis para proteger contra dispositivos potencialmente vulneráveis ou mal-intencionados.

Conforme o STATISTA – portal norte-americano de Estatísticas – estima-se que, até 2020, as indústrias de produtos com alta tecnologia embutida, transporte e logística invistam US\$ 40 bilhões em plataformas, sistemas e serviços de IoT. Globalmente, o comércio B2B – de transação comercial entre empresas – está projetado para investir US\$ 25 bilhões em sistemas IoT, *software* e plataformas dentro de dois anos. Espera-se que o comércio de assistência médica invista US\$ 15 bilhões em IoT<sup>201</sup>.

No entanto, a crescente popularidade da IoT faz dela um caminho tentador para ataques cibernéticos. De fato, de acordo com uma pesquisa feita pelo Gartner – instituto de pesquisa e consultoria de 15.000 organizações em mais de 100 países – quase 20% das empresas pesquisadas observaram pelo menos um

<sup>199</sup> AZAÑA, María Yolanda Sánchez-Urán; RUIZ, María Amparo Grau. **Nuevas Tecnologías y Derecho**. Curitiba: Juruá Editora, 2019, p. 54.

<sup>200</sup> APTHORPE, Noah; REISMAN, Dillon; FEAMSTER, Nick. **A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic**. Cornell University. 18 mai 2017. Disponível em: <https://arxiv.org/abs/1705.06805>. Acesso em: 22 mar. 2020.

<sup>201</sup> STATISTA. **Data storage supply and demand worldwide, from 2009 to 2020 (in exabytes)**. STATISTA. Disponível em: <https://www.statista.com/statistics/751749/worldwide-data-storage-capacity-and-demand/>. Acesso em: 22 mar. 2020.

ataque baseado na IoT nos últimos três anos<sup>202</sup>.

A gigante norte-americana de telecomunicações *Verizon Communications Inc.*, no meio de 2017, enfrentou recentemente violação de dados, em que registros de 14 milhões de clientes foram expostos. Os registros incluíam o nome do cliente, o número do celular e o PIN da conta. Ele também tem endereço residencial, endereço de e-mail e saldo da conta da Verizon. Qualquer pessoa com acesso aos registros poderia, teoricamente, ter violado esses detalhes do assinante<sup>203</sup>.

Em 2015, James Bates, do Arkansas, EUA, foi acusado de assassinar seu amigo que havia sido encontrado morto na banheira de água quente de Bates. O promotor construiu o caso em torno dos dados mantidos no *Amazon Echo* de Bates e em seu medidor inteligente. A *Amazon* se recusou a divulgar os dados coletados pelo Alexa. O caso poderia ter parado naquele momento, mas Bates deu permissão para os dados serem usados durante o processo. O caso foi arquivado em dezembro de 2017, mas a história chegou às notícias e a vida pessoal do réu foi trazida para o domínio público.

Em julho de 2018, foi identificado que cerca de 1,5 milhões de pacientes que visitaram os ambulatórios e policlínicos especializados da SingHealth – de Singapura –, de 1 de maio de 2015 a 4 de julho de 2018, tiveram seus dados pessoais acessados e copiados ilegalmente. Os dados obtidos incluem nome, endereço, sexo, raça e data de nascimento. Informações sobre os medicamentos receitados em ambulatório de cerca de 160.000 desses pacientes também vazaram<sup>204</sup>.

De acordo com os resultados do 2018 *Cost of a Data Breach Study: Global Overview*, lançado pela *IBM Security* e o *Ponemon Institute*, as violações de dados continuam a ser mais caras e resultam em mais registros de consumidores perdidos ou roubados, ano após ano<sup>205</sup>.

---

<sup>202</sup> AZAÑA, María Yolanda Sánchez-Urán; RUIZ, María Amparo Grau. **Nuevas Tecnologías y Derecho**. Curitiba: Juruá Editora, 2019, p. 55.

<sup>203</sup> Ibidem.

<sup>204</sup> Ibidem, p. 56.

<sup>205</sup> PONEMON. **2018 Cost of a Data Breach Study**. Disponível em: <https://www.ibm.com/security/>

Em 2018, o custo total médio de uma violação de dados, o custo médio de cada registro perdido ou roubado (custo per capita) e o tamanho médio das violações de dados aumentaram além das médias do relatório de 2017: (i) o custo total médio subiu de US \$ 3,62 para US \$ 3,86 milhões, um aumento de 6,4%; (ii) o custo médio de cada registro perdido subiu de US\$ 141 para US\$ 148, um aumento de 4,8%; (iii) O tamanho médio das violações de dados aumentou em 2,2%<sup>206</sup>.

No fim de 2018, pesquisadores da americana *PenTestPartners* localizaram uma falha grave em uma câmera de vídeo Swann – IoT – que permitia a um *hacker* visualizar vídeos da câmera de outro usuário. O *hack* foi realmente simples: adicionando um número de série da câmera em um aplicativo, você pode ver a cobertura ao vivo da câmera (os números de série são facilmente acessíveis).

O banco de dados da *SingHealth*, contendo dados pessoais de pacientes e medicamentos dispensados de pacientes ambulatoriais, tem sido alvo de um grande ataque cibernético<sup>207</sup>.

Ademais, estima-se que os gastos mundiais com a IoT atinjam US\$ 745 bilhões em 2019, um aumento de 15,4% sobre os US\$ 646 bilhões gastos em 2018, de acordo com uma nova atualização da *International Data Corporation* (IDC) *Worldwide Semiannual Internet of Things Spending Guide*. A IDC espera que os gastos mundiais em IoT mantenham uma taxa de crescimento anual de dois dígitos ao longo do período de previsão 2017-2022 e ultrapassem a marca de US\$ 1 trilhão

---

data-breach. Acesso: em 22 abr. 2020.

<sup>206</sup> PONEON. **2018 Cost of a Data Breach Study**. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso: em 22 abr. 2020.

<sup>207</sup> A violação de dados pessoais de 1,5 milhão de SingHealth em Singapura em 2018, incluindo o primeiro-ministro Lee Hsien Loong, foi causada por mau gerenciamento do sistema, falta de treinamento dos funcionários e outras falhas importantes, de acordo com o relatório de 454 páginas divulgado hoje [10/01/2019] pelo comitê de investigação. O comitê foi formado logo após a violação de 2018, que incluía as informações pessoais dos pacientes, juntamente com os dados médicos de cerca de 160.000 pacientes. Eles realizaram 22 audiências logo após, revelando que a violação ocorreu cerca de um ano entre agosto de 2017 e julho de 2018. Entre as falhas do *SingHealth*, o comitê encontrou que o Sistema Integrado de Informação em Saúde (IHIS), a agência de TI responsável pelo sistema público de saúde. TI e segurança, careciam de conscientização, recursos e treinamento adequados em segurança cibernética para responder adequadamente ao ataque cibernético” (tradução nossa). In: DAVIS, Jessica. **Massive SingHealth Data Breach Caused by Lack of Basic Security**. Health IT Security. 10 jan. 2019. Disponível em: <https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security>. Acesso em: 20 mar. 2020.

em 2022<sup>208</sup>.

A Diretiva de Proteção de Dados da UE (também conhecida como Diretiva 95/46/EC) foi um regulamento adotado pela União Europeia para proteger a privacidade e proteção de todos os dados pessoais coletados para ou sobre cidadãos da UE, especialmente no que se refere ao processamento, usando ou trocar esses dados.

Dita Diretiva baseia-se em recomendações propostas inicialmente pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE)<sup>209</sup>.

O *Article 29 Working Party* é a designação abreviada em inglês do Grupo de Trabalho para a Proteção de Dados estabelecido pelo artigo 29 dessa Diretiva 95/46/EC. Dito grupo se tornou responsável por fornecer aconselhamento independente sobre problemáticas envolvendo a proteção de dados à Comissão

---

<sup>208</sup> FRAMINGHAM, Mass. **IDC Forecasts Worldwide Spending on the Internet of Things to Reach \$745 Billion in 2019.** Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors. IDC. 3 jan. 2019. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prUS44596319>. Acesso em: 22 mar. 2020.

<sup>209</sup> Conforme a OCDE, tais recomendações se baseiam em 8 princípios: 1. Princípio de Limitação de Coleta: deve haver limites para a coleta de dados pessoais e tais dados devem ser obtidos por meios legais e justos e, quando apropriado, com o conhecimento ou consentimento do titular dos dados; 2. Princípio da Qualidade de Dados: os dados pessoais devem ser relevantes para os propósitos para os quais devem ser usados e, na medida necessária para esses propósitos, devem ser precisos, completos e atualizados; 3. Princípio da Especificação do Propósito: as finalidades para as quais os dados pessoais são coletados devem ser especificadas até o momento da coleta de dados e o uso subsequente limitado ao cumprimento desses propósitos ou outros que não sejam incompatíveis com esses fins e conforme especificado em cada ocasião de mudança de propósito; 4. Princípio da limitação do uso: os dados pessoais não devem ser divulgados, disponibilizados ou utilizados para outros fins que não os especificados em conformidade com o parágrafo 9, exceto: a) com o consentimento do titular dos dados; ou b) pela autoridade da lei; 5. Princípio de Salvaguardas de Segurança: os dados pessoais devem ser protegidos por salvaguardas de segurança razoáveis contra riscos como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados; 6. Princípio da Abertura: deve haver uma política geral de abertura sobre desenvolvimentos, práticas e políticas com relação aos dados pessoais. Os meios devem estar prontamente disponíveis para estabelecer a existência e a natureza dos dados pessoais e os principais objetivos de seu uso, bem como a identidade e a residência habitual do controlador de dados; 7. Princípio da Participação Individual: um indivíduo deve ter o direito: a) obter de um controlador de dados, ou de outra forma, a confirmação de se o controlador de dados possui ou não dados relacionados a ele; b) ter comunicado a ele, dados relativos a ele i) dentro de um prazo razoável; ii) a custo, se houver, que não seja excessivo; iii) de uma maneira razoável; e iv) de uma forma que seja prontamente inteligível para ele; c) ser fundamentado se o pedido feito de acordo com os subparágrafos (a) e (b) for negado, e poder contestar tal negação; e d) contestar os dados relativos a ele para ter os dados apagados, corrigidos, completados ou alterados; 8. Princípio da Responsabilização: um controlador de dados deve ser responsável por cumprir as medidas que dão efeito aos princípios mencionados acima. (tradução nossa)

Europeia, além de auxiliá-la em prol do desenvolvimento de políticas harmonizadas para a proteção de dados nos Estados-Membros da União Europeia<sup>210</sup>.

Posteriormente, a Diretiva de Proteção de Dados foi substituída pelo RGPD, adotado pelo Parlamento Europeu e pelo Conselho Europeu em abril de 2016, se tornando executável em maio de 2018. Esse novo regulamento ampliou os requisitos anteriores para coleta, armazenamento e compartilhamento de dados pessoais e exige que o consentimento do sujeito seja explicitamente afirmado, e não que seja retirado por padrão.

Em outubro de 2016, o *European Data Protection Supervisor* (EDPS), Giovanni Buttarelli, afirmou que o escopo das novas regras de *ePrivacy* precisa ser amplo o suficiente para abranger todas as formas de comunicações eletrônicas, independentemente da rede ou serviço utilizado. De acordo com ele, “os indivíduos devem ter o mesmo nível de proteção para todos os tipos de comunicação, como telefone, aplicativo de mensagens de celular, e Internet das Coisas”<sup>211</sup>.

Essa fala de Buttarelli remete ao documento da EDPS intitulado *Leading by Example: The EDPS Strategy 2015-2019*. Nesse documento, responsável por delinear as estratégias desse órgão europeu em face da regulação da proteção de dados, a Supervisão afirma que pretende incentivar uma conversa mais bem informada sobre o que a IoT e, neste contexto, a inteligência artificial, significará para os direitos digitais. Especificamente sobre esse tema, entre os objetivos estratégicos da EDPS, estão: iniciar um diálogo na União Europeia entre seus organismos e reguladores, acadêmicos, indústria, comunidade de IT, organizações de defesa do consumidor, e outros, sobre Internet das Coisas e direitos fundamentais nos setores público e privado<sup>212</sup>.

---

<sup>210</sup> EUROPEAN DATA PROTECTION SUPERVISOR. **Glossary**. EDPS. Disponível em: [https://edps.europa.eu/data-protection/data-protection/glossary\\_en](https://edps.europa.eu/data-protection/data-protection/glossary_en). Acesso em: 12 mar. 2020.

<sup>211</sup> BUTTARELLI, Giovanni. **ANNEX I – Declaration of Interests**. EDPS. 2016. Disponível em: [https://edps.europa.eu/sites/edp/files/publication/buttarelli\\_di\\_2016\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/buttarelli_di_2016_en.pdf). Acesso em: 22 mar. 2020.

<sup>212</sup> EUROPEAN DATA PROTECTION SUPERVISOR. **Leading by Example: EDPS Strategy 2015-2019**. EDPS. 2 mar. 2015. Disponível em: [https://edps.europa.eu/press-publications/press-news/press-releases/2015/leading-example-edps-strategy-2015-2019\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2015/leading-example-edps-strategy-2015-2019_en). Acesso em: 12 mar. 2020.

Outra ação estratégica é a promoção de uma aliança global com autoridades de privacidade e proteção de dados para identificar respostas técnicas e regulatórias aos principais desafios à proteção de dados<sup>213</sup>.

Ainda no que diz respeito ao RGPD, vale salientar que ele impõe multas sobre a falta de cumprimento em face da proteção de dados. Em primeiro lugar, a empresa pode enfrentar uma penalidade de até 2% de seu faturamento anual, ou 10 milhões de euros, por não comunicar uma violação de dados dentro de 72 horas após tomar conhecimento dela. Essa comunicação deve descrever a natureza dos dados afetados, quantas pessoas aproximadamente são afetadas, quais as consequências para elas e quais medidas já foram tomadas e serão tomadas em resposta à violação<sup>214</sup>.

O PGPD também impõe multa pela violação de dados pessoais em si, sob pena com multa máxima de 4% do faturamento anual da sua empresa, ou 20 milhões de euros, o que for maior<sup>215</sup>.

No Brasil, dentre outras cidades, Joinville, no Estado de Santa Catarina, implantou em agosto de 2017 sua primeira antena de rede de Internet das Coisas. Conforme dados da própria prefeitura:

Uma vez instalada, a antena poderá cobrir área de 40 km de raio a partir do seu entorno. Inicialmente, a rede gratuita será utilizada pelas universidades em pesquisas e desenvolvimento. Futuramente, o objetivo é cobrir toda a cidade com uma rede dedicada à IoT, que tem como conceito principal operar com muito baixo custo e consumo mínimo de energia e bateria<sup>216</sup>.

Uma empresa brasileira especializada em IoT, vinculada à proposta de Joinville, afirmou que a iniciativa da cidade permite transformar qualquer câmera de segurança analógica ou IP em equipamentos de vigilância que geram dados importantes para a segurança pública. “Com o uso de ferramentas de inteligência

<sup>213</sup> EUROPEAN DATA PROTECTION SUPERVISOR. **Leading by Example**: EDPS Strategy 2015-2019. EDPS. 2 mar. 2015. Disponível em: [https://edps.europa.eu/press-publications/press-news/press-releases/2015/leading-example-edps-strategy-2015-2019\\_en](https://edps.europa.eu/press-publications/press-news/press-releases/2015/leading-example-edps-strategy-2015-2019_en). Acesso em: 12 mar. 2020.

<sup>214</sup> AZAÑA, María Yolanda Sánchez-Urán; RUIZ, María Amparo Grau. **Nuevas Tecnologías y Derecho**. Curitiba: Juruá Editora, 2019, p. 60.

<sup>215</sup> Ibidem.

<sup>216</sup> PREFEITURA DE JOINVILLE. **Instalada 1ª antena de rede de Internet das Coisas em Joinville**. Joinville. 23 ago. 2017. Disponível em: <https://www.joinville.sc.gov.br/noticias/instalada-1a-antena-de-rede-de-internet-das-coisas-em-joinville/>. Acesso em: 22 mar. 2020.



artificial, mais especificamente visão computacional, o sistema pode identificar padrões de carros, placas, rostos e movimentos para melhorar a capacidade de monitoramento”<sup>217</sup>.

Além de Joinville, outras cidades brasileiras estão se adequando aos sistemas de IoT. Por exemplo, para melhoria na gestão do trânsito da cidade, a Prefeitura Municipal de São Paulo estabeleceu uma parceria entre a Companhia de Engenharia de Tráfego e a empresa de aplicativo de trânsito Waze:

Com o acordo, o Waze vai repassar automaticamente à CET as informações sobre semáforos quebrados que estiverem disponíveis em sua plataforma – nela, os usuários reportam obstáculos em tempo real, o que permite ao aplicativo traçar a melhor rota para o motorista chegar ao seu destino<sup>218</sup>.

Além disso, no Brasil algumas seguradoras estão desenvolvendo sistemas para monitorar os clientes quando se envolvem em acidentes de carro. E isso através de imagens e sons capturados por câmeras e sensores da própria cidade. Essa tecnologia terá a capacidade de avisar a seguradora sobre o sinistro, auxiliando o motorista no envio de ajuda antes mesmo dele ter que acionar pessoalmente a seguradora<sup>219</sup>.

Especificamente no Brasil, há um amplo debate sobre a relação entre a Lei 12.965/2014 e a regulamentação da IoT. E isso porque entra em discussão a questão da neutralidade da rede, prevista tanto no art. 3º, inc. IV, quanto na Seção I do Capítulo III, ambos dessa lei do MCI: “Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios: [...] IV – preservação e garantia da neutralidade de rede”<sup>220</sup>.

---

<sup>217</sup> ALIGER. **Aumentar a eficiência, diminuir os custos e sustentar a vantagem competitiva**. 2019. Disponível em: <https://www.aliger.com.br/>. Acesso em: 22 mar. 2020.

<sup>218</sup> BASILIO, Patricia. Como a internet das coisas já mudou algumas das maiores cidades do mundo. **Época Negócios**. 2018. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/12/como-internet-das-coisas-ja-mudou-algumas-das-maiores-cidades-do-mundo.html>. Acesso em: 22 mar. 2020.

<sup>219</sup> Ibidem.

<sup>220</sup> A neutralidade de rede baseia-se no princípio de que todas as informações que trafegam na rede devem ser tratadas da mesma forma, navegando à mesma velocidade, garantindo o livre acesso a qualquer tipo de conteúdo na rede sem ferir a autonomia do usuário e não discriminar determinadas aplicações por consumo de banda larga (AZAÑA; RUIZ, 2019).

É possível se afirmar que, com a implantação das redes de IoT, haverá possivelmente a demanda para a flexibilização da neutralidade da rede. Nesse caso, é importante reforçar que o Marco Civil da Internet, no seu art. 9º, § 1º, já afasta a aplicabilidade da regra de neutralidade da rede a alguns casos ao dizer que a discriminação de tráfego está permitida quando existirem: “I – requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II – priorização de serviços de emergência”<sup>221</sup>.

Desse modo, preocupações acerca das chamadas aplicações IoT de missão crítica (como algumas aplicações IoT no ambiente de saúde), já podem ser enfrentadas e tratadas com base no quadro normativo atual do MCI

Por outro lado, há o Decreto 8.771/2016, regulando, entre outras coisas, o art. 9º do MCI, como, por exemplo, o referido inc. I desse art. 9º, o qual enuncia de forma abrangente que esta discriminação de tráfego é permitida nos casos em que existirem “requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações”<sup>222</sup>. Esse decreto diz que esse inciso se aplica:

[...]

II – aos serviços especializados, entendidos como serviços otimizados por sua qualidade assegurada de serviço, de velocidade ou de segurança, ainda que utilizem protocolos lógicos TCP/IP ou equivalentes, desde que: a) não configurem substituto à internet em seu caráter público e irrestrito; e b) sejam destinados a grupos específicos de usuários com controle estrito de admissão<sup>223</sup>.

As principais perguntas que remanescem: Será possível enquadrar parte das IoT como “serviços otimizados por sua qualidade assegurada de serviço”? É possível dizer que um grupo de consumidores de determinado produto, mesmo sendo esse produto constituído de um contrato de adesão e requisitando o aceite ou não do usuário, é considerado um “grupo específico de usuários com controle estrito de admissão”? Se sim, para uma ou ambas as perguntas, estarão os sistemas e produtos de IoT ausentes de compromisso com a neutralidade de rede?

---

<sup>221</sup> BRASIL. **Lei n. 12.965 de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 25 mar. 2020.

<sup>222</sup> Ibidem.

<sup>223</sup> Ibidem.

Outro ponto a se salientar é que o Marco Civil da Internet não cita em nenhum momento especificamente a IoT. Há apenas sua menção no Decreto 9.319/18, responsável por instituir o Sistema Nacional para a Transformação Digital e a Estratégia Brasileira para a Transformação Digital – *E-Digital*.

Dentre as diretrizes do Anexo I desse Decreto, o qual trata dos chamados Eixos Temáticos da *E-Digital*, está enunciado que, “ao reconhecer o potencial transformador das aplicações da Internet das Coisas, devem ser estabelecidos ações e incentivos destinados à contínua evolução e disseminação dos dispositivos e das tecnologias digitais associadas”<sup>224</sup>.

Ademais, há também o debate sobre a classificação jurídica da internet das coisas. E suas ramificações são relevantes, por exemplo, na questão tributária: se classificada a internet das coisas, como “serviço de valor adicionado”, haverá possivelmente a tributação municipal por ISS. Por outro lado, se a internet das coisas for classificada como “serviço de telecomunicações”, haverá a incidência da tributação estadual por ICMS.

Há, ainda, alguns projetos de lei com o intuito de afastar a cobrança de taxas e contribuições sobre as estações de IoT (ambientes de controle, monitoramento, coleta de dados etc.). É o caso do Projeto de Lei 7.656/17.

Já o projeto de lei substitutivo a esse, atribui à Anatel a competência para definir o conceito de comunicação máquina a máquina, para a aplicação de isenção da tributação pela contribuição para o fomento da radiodifusão pública e da isenção pela contribuição para o desenvolvimento da indústria cinematográfica. E isso, apesar de que, tecnicamente, a lei deva definir este conceito. É isso o que impõe o princípio da estrita legalidade tributária.

Assim, entende-se ser necessária a criação da Autoridade Nacional de Proteção de Dados (ANPD) no plano nacional da IoT.

---

<sup>224</sup> BRASIL. **Decreto n. 9.319, de 21 de março de 2018**. Institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Decreto/D9319.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9319.htm). Acesso em: 25 mar. 2020.

Em maio de 2014, foi promulgado o Decreto 8.234/2014, o qual foi o responsável por estipular as características e formação da Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas Máquina a Máquina, essa efetivamente criada pela Portaria 1.420/2014.

Conforme o diretor de Banda Larga do Ministério das Comunicações, Artur Coimbra, estão entre os objetivos da Câmara: 1) acompanhar a evolução e o surgimento de novas aplicações máquina a máquina; 2) coordenar a cooperação técnica entre prestadoras de serviços de telecomunicações, fabricantes de equipamentos e entidades de pesquisa; e 3) os seus integrantes vão trabalhar na formulação de políticas públicas para o setor<sup>225</sup>.

Conforme a Portaria que estabeleceu a sua criação, é a Secretaria de Telecomunicações do Ministério das Comunicações quem prestará o apoio administrativo aos trabalhos da Câmara.

Já em dezembro de 2018, veio a Medida Provisória 869, que cria, como órgão da administração pública federal, a ANPD, estabelecendo sua composição e suas competências e garantindo sua autonomia técnica.

A criação da Autoridade estava prevista na LGPD. De acordo com a referida Medida Provisória que cria a ANPD, ela pode ser acionada pelo titular dos seus dados, mediante petição, em relação aos dados do titular por ele tratados, a obter do controlador: acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; entre outros.

A ANPD é ligada à Presidência da República e conta com um conselho diretor composto por cinco diretores, incluindo o presidente. A função principal da ANPD é fiscalizar o recolhimento e a transmissão de dados pessoais dos cidadãos por instituições públicas e privadas. Essa Medida Provisória, que criou a ANPD, ainda precisa da apreciação pelo Congresso Nacional para se converter

---

<sup>225</sup> BRASIL. Ministério das Comunicações. **Governo instaura Câmara de Gestão para comunicações máquina a máquina**. 22 dez. 2017. Disponível em: <http://www.brasil.gov.br/noticias/infraestrutura/2014/10/governo-instaura-camara-de-gestao-para-comunicacoes-maquina-a-maquina>. Acesso em: 22 mar. 2020.

definitivamente em lei ordinária. Por conta da ausência até o momento de manifestação do Congresso, tem-se, então, dois cenários:

1) um relativo especificamente aos sistemas máquina à máquina, o qual corresponde à Portaria 1.420/2014 (Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas Máquina a Máquina), e que estabelece enunciados muito mais relativos às aplicações e os processos de IoT em si; e

2) outro que diz respeito muito mais aos sistemas de recolhimento e a transmissão de dados pessoais dos cidadãos por instituições públicas e privadas – ANPD (Lei n. 13.709/18 – e Medida Provisória 869).

Importante dizer que, na parte em que trata da Viabilidade Econômica (art. 5º, § 6º), a Portaria 1.420/2014, que cria a Câmara de Gestão, enuncia que se buscará:

a) atuar para que os recursos necessários à implementação das diversas iniciativas estejam disponíveis; b) promover programas de financiamento com cooperação entre empresas grandes, médias e pequenas, bem como com ICTs; c) viabilizar instrumentos financeiros estruturados com risco compatível para projetos cooperativos de desenvolvimento, inovação e engenharia relacionados à IoT; d) avaliar o custo das soluções nos ambientes priorizados e propor mecanismos que removam barreiras econômicas e financeiras<sup>226</sup>.

Ou seja, de acordo com esses enunciados dessa Portaria, é absolutamente relevante a necessidade de integrar as normativas da Portaria com a da Medida Provisória (se vier a ser aprovada) e a Lei de Proteção de Dados Pessoais (13.709/18), em outras palavras, que a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas Máquina a Máquina e a ANPD se dialoguem de forma harmoniosa entre si, tendo em vista uma regulamentação mais integral, completa e específica sobre a Internet das Coisas e, conseqüentemente sobre a inteligência artificial.

---

<sup>226</sup> BRASIL. **Portaria 1.420, de 8 de outubro de 2014**. Cria a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=55&data=09/10/2014>. Acesso em: 25 mar. 2020.

Referente à questão da proteção dos dados, no Brasil a LGPD é relativamente nova e são poucos os julgados posteriores à legislação. Ainda não é possível afirmar incisivamente, com base na pequena construção jurisprudencial posterior a esta legislação, se com o advento da nova lei observa-se maior proteção à privacidade. Veja-se, neste sentido, um acórdão que se refere ao vazamento de dados de um consumidor:

APELAÇÃO CÍVEL - AÇÃO ANULATÓRIA DE CONTRATO E INDENIZAÇÃO POR DANOS MORAIS - CONTRATAÇÃO DE EMPRÉSTIMOS - CAIXA ELETRÔNICO - CULPA EXCLUSIVA DA VÍTIMA - NÃO CONFIGURADA - DEFEITO NA PRESTAÇÃO DO SERVIÇO BANCÁRIO - VAZAMENTO DE DADOS PESSOAIS - DANOS MORAIS CARACTERIZADOS - QUANTUM INDENIZATÓRIO - ADEQUAÇÃO DEVIDA - SENTENÇA REFORMADA EM PARTE. [...] Reveste-se de ilicitude a hipótese em que a instituição financeira permite ou não cuida para impedir o vazamento dos dados pessoais de seus clientes oportunizando, assim, a atuação ilícita de terceiros fraudadores<sup>227</sup>.

Veja-se que este julgado foi favorável ao consumidor e contrário à instituição bancária que deixou vazar dados pessoais de um cliente, o que oportunizou que este fosse vítima de uma fraude.

Por fim, importa citar um caso que ocorreu recentemente envolvendo a empresa holandesa C&A<sup>228</sup>, que opera também no Brasil. Referida empresa, quinze dias após o presidente sancionar a LGPD protagonizou um maciço vazamento de dados de seus clientes, dados estes obtidos junto aos mesmos nas diversas lojas distribuídas no Brasil, quando os clientes são abordados por vendedores e induzidos a fazer um cartão de crédito da loja. Esta é uma prática, aliás, bastante comum em lojas âncoras, como é o caso também das Lojas Pernambucanas, Renner, Riachuelo, dentre outras.

Referente à C&A, denúncias foram realizadas acusando a empresa de fazer uso de informações coletadas de pessoas que se candidataram às vagas de emprego para que fossem emitidos cartões não solicitados. No dia 30 de agosto de

<sup>227</sup> MINAS GERAIS. Tribunal de Justiça de Minas Gerais. **AC 1.0471.16.012594-7/001**. Relatora: Desa. Juliana Campos Hora, 12ª Câmara Cível, Dje. 08/08/2019. Disponível em: <http://www.idealsoftwares.com.br/idealnewsjd/noticia.php?id=7937>. Acesso em: 18 mar. 2020.

<sup>228</sup> FLIPSIDE. **Caso C&A**: o que muda com a Lei Geral de Proteção de Dados? 03.09.2018. Disponível em: <https://www.flipside.com.br/blog/2018/9/2/caso-cea-o-que-muda-com-a-lgpd>. Acesso em: 18 mar. 2020.

2018, foram vazados os endereços eletrônicos de clientes e funcionários da empresa, supostamente com o intuito de retaliar a denúncia. À época, um perfil do Twitter assumiu a autoria do feito.

Segundo expõe o site Flipside<sup>229</sup>, não se sabe a época em que o sistema foi invadido, no entanto vários registros do sistema de vendas de cartão da empresa foram divulgados. O grupo que assumiu a autoria do feito afirmou que teve acesso a cerca de 36 mil dados cadastrais, incluindo nome, CPF e RG.

Neste caso, por exemplo, se a LGPD já estivesse em vigor à época dos ataques, todos os usuários afetados pelo incidente deveriam ser notificados pela empresa, o que desencadearia uma quebra de confiança e mácula na imagem da empresa junto aos clientes. Ademais, se ficasse comprovado que o vazamento ocorreu em razão de negligência (a exemplo de desatualização do sistema ou uso de senhas fracas), são previstas sanções pela legislação que podem ir, conforme a gravidade do incidente, desde advertências a multas que podem chegar a até 50 milhões de reais ou 2% do faturamento anual da empresa.

Não obstante a C&A ser uma empresa holandesa, a lei aplicada a este caso é a brasileira, exceto se existirem vítimas cuja nacionalidade seja a européia. Neste último caso, a lei aplicada seria a RGPD e as multas teriam o dobro do valor previsto na legislação do Brasil.

Assim, o que se percebe é que o caso concreto é que ditará a sanção que será aplicada. Decerto que aparecerão situações que irão suscitar dúvidas e questionamentos, mas a construção doutrinária, jurisprudencial e até mesmo legislativa se incumbirá de tratar destas lacunas à medida que estas forem surgindo.

Do exposto é possível constatar que apesar de não ter havido tempo para a formação de uma construção jurisprudencial baseada nesta nova lei, a perspectiva social leva a crer que posicionamento jurisprudencial dominante, com o advento da

---

<sup>229</sup> FLIPSIDE. **Caso C&A:** o que muda com a Lei Geral de Proteção de Dados? 03.09.2018. Disponível em: <https://www.flipside.com.br/blog/2018/9/2/caso-cea-o-que-muda-com-a-lgpd>. Acesso em: 18 mar. 2020.

Lei n.13.709/2018 deverá se esforçar para que o direito à privacidade seja resguardado, sem, no entanto, obstar o desenvolvimento da tecnologia da informação.



## CONSIDERAÇÕES FINAIS

O privado e o público são âmbitos paradoxais, porém de estreita relação e em prováveis situações de conflito. A relação entre esses dois âmbitos na Era da Informação mudou significativamente, no sentido de tornar pública algumas situações que ocorriam no âmbito privado.

As instituições públicas e privadas do mundo contemporâneo têm oferecido, por intermédio da tecnologia da informação, utilidades para as mais diversas necessidades humanas, com destaque para aquelas relacionadas com a informação, a comunicação, o consumo e os serviços públicos em geral.

As tecnologias da informação e da comunicação estão a cada dia se tornando necessárias para as mais diversas atividades humanas, devido à maneira como as instituições públicas e privadas, bem como a sociedade, estão se estruturando, seja em função das políticas públicas implementadas, seja para atender objetivos de instituições privadas ou até interesses pessoais.

O elenco dos direitos fundamentais previstos na Constituição da República Federativa do Brasil que têm estreita relação com a proteção dos dados pessoais e, por consequência, da privacidade, diz respeito: à intimidade, à vida privada, à imagem das pessoas, a casa, às comunicações de todos os tipos, mediante correspondência tradicional (carta) ou eletrônica (e-mail), telefônica (voz, ou mensagens eletrônicas), de dados, e telegráfica. Essa relação passou a ser mais intensa em face do avanço tecnológico nessa era chamada de sociedade da informação.

O direito fundamental à proteção de dados pessoais protege a privacidade, um dos direitos da personalidade. Aquela, a seu turno, engloba a intimidade e a vida privada, na perspectiva da teoria dos círculos concêntricos que, não obstante ser atualmente abominada pela doutrina que a originou, serve de esquema para estruturação da relação entre os atos da pessoa e a tutela de sua privacidade.

Dados pessoais não podem ser vistos simplesmente como informação que compõe dados estatísticos ou até mercadoria a ser negociada. Deve ser visto como um dos componentes da personalidade que deve ser protegido em termos diferentes do que já foi feito até então.

Nesse cenário de avanço tecnológico, dados pessoais que necessitam de proteção jurídica podem ser uma imagem, uma conversa, uma filmagem, hábitos de consumo pessoal, registrados por meio de operações via Internet ou administradoras de cartões de crédito, dentre outras informações. As possibilidades são as mais diversas, principalmente devido tudo estar interconectado, como é o caso da Internet das Coisas, tendo em vista as circunstâncias sociais, mercadológicas e tecnológicas atuais.

A perda da privacidade é muito maior do que se imagina e do que se divulga. Os avanços nas técnicas de pesquisa inteligente de dados e de formação de base de dados estratosféricas demonstram que a expansão da rede é algo ilimitado. Os sistemas proporcionam a revelação de muitos aspectos da privacidade sem o conhecimento e consentimento da pessoa alvo, com base em informações pessoais mínimas existentes na rede.

É de suma importância a compreensão dos interesses subjacentes de toda essa superestrutura. Isso demanda uma visão sistêmica que consiste em ampliar o foco de observação, contextualizar o fenômeno e focalizar as interações recursivas. Juridicamente significa garantir o acesso mais amplo possível a todas as informações socialmente relevantes, públicas e privadas, por meio de uma nova geração de leis sobre o acesso às informações, mediante os mais diversos recursos tecnológicos; impedir que as coletas de dados pessoais se transformem em instrumentos de discriminação ou retaliação política; e reagir a qualquer forma de transformação da pessoa humana em número ou mercadoria.

Apesar de o Brasil fazer parte da Rede Ibero-Americana de Proteção de Dados (RIPD), a legislação sobre essa proteção ainda é incipiente, bem como a cultura jurídica do país ainda está mais voltada para a discussão das políticas públicas relativas ao mínimo existencial, porque grande parte da população ainda

carece de tais condições. Porém, não é de menos importância a proteção de outros direitos fundamentais, a exemplo dos que dizem respeito à privacidade, principalmente porque a informação tornou-se um bem de valor econômico incomensurável para determinadas instituições públicas ou privadas, uma riqueza fundamental da sociedade.

O MCI se limitou a proteção dos dados pessoais, quando previu a tutela somente para usuários da Internet. Tal tutela de direitos não deve ser somente do usuário, mas de qualquer pessoa. Há diversas situações nas quais a pessoa não é usuária da Internet momentaneamente, porém fatos que dizem respeito à sua privacidade são capturados, arquivados e processados na rede, sem que o titular desses dados tenha conhecimento. Com efeito, crê-se que o sistema legal de proteção de dados pessoais do país está muito aquém para ter efetividade, devido à falta de políticas públicas eficazes para essa proteção.

O direito à autodeterminação informativa surge como consectário do direito fundamental à proteção de dados pessoais, em face da tecnologia da informação. Tal direito considera ilegítima toda coleta de informações pessoais que seja realizada sem o prévio conhecimento e explícito consentimento da pessoa. Consiste ainda que determinadas informações coletadas não devem circular fora da instituição pública ou privada que tenha coletado essas informações originalmente para certa finalidade.

A LGPD ingressa tardiamente no ordenamento pátrio, mas visa à proteção de dados pessoais do indivíduo. Para isso trouxe diversos fundamentos relacionados com a personalidade, especialmente o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Esses fundamentos estão intimamente ligados à cidadania do novo milênio.

A ampla liberdade de expressão é alvo de duras críticas, sobretudo, por não garantir, deveras, uma igualdade no exercício deste direito, diante de sociedades marcadas por disparidades sociais e econômicas em que determinadas

grupos não têm as mesmas oportunidades de acesso aos meios de comunicação e as classes mais privilegiadas conquistam o campo da verdade com suas ideias, interesses e necessidades.

Este cenário contribui ainda para o desenvolvimento da intolerância e, por conseguinte, para a disseminação da desigualdade e da discriminação de determinados grupos sociais, o que gradualmente, resulta nos casos de discursos do ódio, que se encontra mais próximo do ataque do que da participação e debate, em que manifestações tem como exclusivo intuito insultar, discriminar e estigmatizar, desvalorizar, incitar a violência ou humilhar determinado grupo como um todo ou os indivíduos que o compõe, negando um estatuto de igualdade às suas vítimas.

Dito isto, é possível concluir que não obstante o tratamento jurídico dispensado aos dados pessoais dos cidadãos no Brasil não tenha sido suficiente para resguardar o direito fundamental à privacidade em tempos de massificação dos dados, o posicionamento jurisprudencial dominante antes do advento da Lei n.13.709/2018 se esforçava em assegurar que o direito à privacidade fosse resguardado, sem, no entanto, obstar o desenvolvimento da tecnologia da informação e entende-se que o desejável é que a jurisprudência caminhe nesta direção, ou seja, combatendo os excessos, protegendo o direito à privacidade, sem, no entanto, incorrer no risco de instituir a censura.

Assim, apesar de ainda não se vislumbrar uma quantidade significativa de julgados após o advento da Lei n.13.709/2018, visto tratar-se de uma Lei recente e que ainda entrará em vigor em agosto de 2020, espera-se que seja levada em conta a necessidade de proteger esse direito, sempre levando em conta que na era da evolução tecnológica em que se vive, os “dados são o novo petróleo”, essenciais ao desenvolvimento de qualquer país, visto que estão ligados às tecnologias que fazem a diferença no mundo moderno atual.

O desafio mostra-se imenso, mas percebe-se que o Brasil caminha e dá seus passos no sentido de proteger os dados dos seus cidadãos, ao mesmo tempo em que permite a continuação da evolução tecnológica pela qual se passa atualmente. No entanto, para que essa efetividade aconteça, é necessária a

realização de políticas públicas, a exemplo da criação de plataformas educacionais com vistas à educação e conscientização da sociedade.

As empresas brasileiras e os cidadãos precisam assimilar a cultura da proteção de dados pessoais e devem entender o direito à privacidade como um princípio e não como uma obrigação. É princípio da lei o desenvolvimento econômico e a inovação e não apenas a proteção de dados. Então não se pode permitir que certas atividades inovadoras sejam impedidas pela LGPD. O que é preciso (e está na lei) é estabelecer responsabilidades para essas pessoas que querem avançar, que querem desenvolver o país, mas que agora, com a LGPD precisarão fazer isso de forma responsável, levando em conta as boas práticas, com governança e segurança.

Portanto, com a positivação dessa norma/direito e a conscientização e educação da sociedade quanto ao tema, o direito será capaz - como já vem se esforçando - de responder às novidades propostas pela tecnologia da informação, com a realização do seu valor fundamental: a pessoa humana e sua dignidade.

## REFERÊNCIA DAS FONTES CITADAS

ALEX, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008. (Coleção teoria & direito público).

ALIGER. **Aumentar a eficiência, diminuir os custos e sustentar a vantagem competitiva**. 2019. Disponível em: <https://www.aliger.com.br/>. Acesso em: 22 mar. 2020.

APTHORPE, Noah; REISMAN, Dillon; FEAMSTER, Nick. **A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic**. Cornell University. 18 mai 2017. Disponível em: <https://arxiv.org/abs/1705.06805>. Acesso em: 22 mar. 2020.

ASSANGE, Julian. **Cypherpunks: Liberdade e o Futuro da Internet**. São Paulo: Boitempo, 2013.

ÁVILA, Humberto. **Teoria dos Princípios**. 18. ed. São Paulo: Malheiros, 2018.

AZAÑA, María Yolanda Sánchez-Urán; RUIZ, María Amparo Grau. **Nuevas Tecnologías y Derecho**. Curitiba: Juruá Editora, 2019.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. São Paulo: Saraiva, 2009.

BAUMAN, Z. **O mal-estar da pós-modernidade**. Tradução Mauro Gama; Cláudia Martinelli Gama. Rio de Janeiro: Zahar, 1998.

BITTENCOURT, G. **Inteligência artificial: ferramentas e teorias**. 2. ed. Florianópolis: Editora da UFSC, 2001.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 33. ed. São Paulo: Malheiros, 2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm). Acesso em: 21 Fev. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 25 Fev. 2020.

BRASIL. Ministério das Comunicações. **Governo instaura Câmara de Gestão para comunicações máquina a máquina**. 22 dez. 2017. Disponível em: <http://www.brasil.gov.br/noticias/infraestrutura/2014/10/governo-instaura-camara-de-gestao-para-comunicacoes-maquina-a-maquina>. Acesso em: 22 mar. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). 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: 22 jan. 2020.

BUTTARELLI, Giovanni. **ANNEX I – Declaration of Interests.** EDPS. 2016. Disponível em: [https://edps.europa.eu/sites/edp/files/publication/buttarelli\\_di\\_2016\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/buttarelli_di_2016_en.pdf). Acesso em: 22 mar. 2020.

BREGA FILHO, Vladimir. **Direitos fundamentais na Constituição de 1988:** conteúdo jurídico das expressões. São Paulo: Juarez de Oliveira, 2002.

CABÉ, Benjamin. **Key trends from the IoT Developer Survey 2018.** Blog Benjamin Cabé. 17 abr. 2018. Disponível em: <https://blog.benjamin-cabe.com/2018/04/17/key-trends-iot-developer-survey-2018>. Acesso em: 22 mar. 2020.

CANOTILHO, J.J. Gomes; MACHADO, Jónatas E.M. **“Reality Shows” e Liberdade de Programação.** Coimbra: Coimbra Editora, 2003.

CARVALHO, Ana Cristina Azevedo. **Marco Civil da Internet no Brasil.** São Paulo: Editora Alta Books, 2014.

CARVALHO, Osvaldo Ferreira de. **Restrições aos Direitos Fundamentais no Estado Constitucional.** Curitiba: Juruá Editora, 2019.

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

CASTRO, Nuno Teixeira. Um novo quadro legal europeu em matéria de proteção de dados vislumbrando o Mercado Único Digital para a Europa. **Diário Insónias.** [S.l.], 11.05.2016. Disponível em: <http://www.insonias.pt/um-novo-quadro-legal-europeu-materia-proteccao-dados-vislumbrando-mercado-unico-digital-europa/amp/>. Acesso em: 20 Fev. 2020.

CEBRIÁN, Juan Luis. **A Rede:** como nossas vidas serão transformadas pelos novos meios de comunicação. Lisboa: Summus, 1999.

COMITÊ GESTOR DA INTERNET NO BRASIL. **A internet e o TCP IP. IPv6.** 15 mai. 2012. Disponível em: <http://ipv6.br/post/introducao/>. Acesso em: 12 mar. 2020.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS. **10 medidas para preparar a aplicação do Regulamento Europeu de Proteção de Dados.** [S.l.], 28.01.2017. Disponível em: [https://www.cnpd.pt/bin/rgpd/10\\_Medidas\\_para\\_preparar\\_RGPD\\_CNPd.pdf](https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPd.pdf). Acesso em: 23 Fev. 2020.

CRUZ, Paulo Márcio; SALLES, Alice Francisco da Cruz. Considerações sobre os direitos fundamentais sociais prestacionais e a sua concretização pelo poder judiciário. **Revista Eletrônica Direito e Política**, Programa de Pós Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.6, n.3, 2011. Disponível em:

[www.univali.br/direitoepolitica](http://www.univali.br/direitoepolitica). Acesso em: 8 abr. 2020.

DAVIS, Jessica. **Massive SingHealth Data Breach Caused by Lack of Basic Security**. Health IT Security. 10 jan. 2019. Disponível em: <https://healthitsecurity.com/news/massive-singhealth-data-breach-caused-by-lack-of-basic-security>. Acesso em: 20 mar. 2020.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 3. ed. rev. atual. e ampl. São Paulo: RT, 2011.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DOYLE, Daniella. **O que é Big Data e por que é tão valioso para sua empresa?** 2020. Disponível em: <https://www.siteware.com.br/gestao-estrategica/o-que-e-big-data/>. Acesso em: 8 Mar. 2020.

DUQUE, Marcelo Schenk. **Curso de direitos fundamentais: teoria e prática**. São Paulo: Revista dos Tribunais, 2014.

DWORKIN, Ronald. **Levando os Direitos a sério**. São Paulo: Martins Fontes, 2002.

EUROPEAN Data Protection Supervisor. **Glossary**. EDPS. Disponível em: [https://edps.europa.eu/data-protection/data-protection/glossary\\_en](https://edps.europa.eu/data-protection/data-protection/glossary_en). Acesso em: 12 mar. 2020.

FERGUSON, Andrew Guthrie. Big Data and Predictive Reasonable Suspicion. **Univesity of Pensylvania Law Review**, v. 163, n. 327, January, 2015.

FLIPSIDE. **Caso C&A: o que muda com a Lei Geral de Proteção de Dados?** 03.09.2018. Disponível em: <https://www.flipside.com.br/blog/2018/9/2/caso-cea-o-que-muda-com-a-lgpd>. Acesso em: 18 mar. 2020.

FLORENCIO, Juliana Abrusio. **Proteção de dados na cultura do algoritmo**. Tese (Doutorado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica de São Paulo, São Paulo, 2019.

FORTES, Vinícius Borges. **Os Direitos de Privacidade e a Proteção de Dados Pessoais na Internet**. Rio de Janeiro: Lumen Juris, 2016.

FRAMINGHAM, Mass. **IDC Forecasts Worldwide Spending on the Internet of Things to Reach \$745 Billion in 2019**. Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors. IDC. 3 jan. 2019. Disponível em: <https://www.idc.com/getdoc.jsp?containerId=prUS44596319>. Acesso em: 22 mar. 2020.

FREIRE, Alexandre. **Inevitável Mundo Novo: O Fim da Privacidade**. São Paulo: Axis Mundi, 2006.



FREITAS JR., José Carlos da Silva; MAÇADA, Antônio Carlos Gastaud; OLIVEIRA, Mirian et al. Big Data e gestão do conhecimento: definições e direcionamentos de pesquisa. **Revista Alcance**, v.23, n.4, p.529-546, 2016.

GAMIZ, Mario Sergio de Freitas. **Privacidade e Intimidade**. Curitiba: Juruá Editora, 2012.

GILISSEN, J. **Introdução histórica ao direito**. Tradução A. M. Botelho Hespanha e L. M. Macaísta Malheiros. 4. ed. Lisboa: Fundação Calouste Gulbenkian, 2003.

GUIDI, Guilherme Berti de Campos. **Modelos regulatórios para proteção de dados pessoais**. 2017. Disponível em: <https://itsrio.org/wpcontent/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf>. Acesso em: 23 Fev. 2020.

LEAL, Luziane de Figueiredo Simão. **Crimes Contra os Direitos da Personalidade na Internet**. Curitiba: Juruá Editora, 2015.

LEITE, Eduardo de oliveira. **A monografia jurídica**. 5 ed. São Paulo: Revista dos Tribunais, 2001.

LEMOALLE, Edouard; CARBONI, Guilherme. **Lei Europeia de Proteção de Dados Pessoais (GDPR) e seus efeitos no Brasil**. JOTA. [S.l.], 12.02.2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018>. Acesso em: 23 Fev. 2020.

LEMONS, A. **Cibercultura: tecnologia e vida social na cultura contemporânea**. Porto Alegre: Sulina, 2002.

LIMBERGER, Têmis. **O Direito à Intimidade na Era da Informática**. Porto Alegre: Livraria do Advogado, 2007.

LONGHI, João Victor Rozatti. **Processo Legislativo Interativo**. Curitiba: Juruá Editora, 2017.

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

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova: A Investigação Criminal em Busca da Verdade**. 2. ed. Curitiba: Juruá Editora, 2015.

MARQUES, J; SILVA, M.F. **O Direito na Era digital**. Porto Alegre: Livraria do Advogado Editora, 2012.

McDOWELL, J. **Mente y mundo**. Trad. Miguel Angel Quintana. Salamanca: Ediciones Sígueme, 2003.

MÊLO, Augusto. **Proteção de Dados Pessoais na Era da Informação**. Curitiba: Juruá Editora, 2019.

MENDES, Alexandre José; ROSA, Alexandre Moraes da; ROSA, Izaias Otacílio da. Testando a *Methodology Multicriteria Decision Aid – Constructivist* (MCDA-C) na construção de algoritmos de apoio à estabilidade das decisões judiciais. **Revista Brasileira de Direito**, Passo Fundo, v. 15, n. 2, p. 281-305, Mai-Ago, 2019.

MINAS GERAIS. Tribunal de Justiça de Minas Gerais. **AC 1.0471.16.012594-7/001**. Relatora: Desa. Juliana Campos Hora, 12ª Câmara Cível, Dje. 08/08/2019. Disponível em: <http://www.idealsoftwares.com.br/idealnewsjd/noticia.php?id=7937>. Acesso em: 18 mar. 2020.

MURRAY, J. **Hamlet on the holodeck**: the future of narrative in cyberspace. Cambridge/Londres: MIT, 1997.

NETHER, Nicholas Augustus de Barcellos. **Proteção de Dados dos Usuários de Aplicativos**. Curitiba: Juruá Editora, 2018.

NOVAIS, Jorge Reis. **As Restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição**. Coimbra: Coimbra Editora, 2003.

PASOLD, Cesar Luiz. **Função Social do Estado Contemporâneo**. 4 ed. Itajaí: Univali, 2013.

PASOLD, Cesar Luiz. **Metodologia da pesquisa jurídica**: teoria e prática. 13 ed. Florianópolis: Conceito Editorial, 2015.

PENROSE, R. **Shadows of the mind**: a Search for the Missing Science of Consciousness. Oxford: University Press, 1994.

PEREIRA, Jane Reis Gonçalves. **Interpretação constitucional e direitos fundamentais**: uma contribuição ao estudo das restrições aos direitos fundamentais na perspectiva da teoria dos princípios. Rio de Janeiro: Renovar, 2006.

PONEMON. **2018 Cost of a Data Breach Study**. Disponível em: <https://www.ibm.com/security/data-breach>. Acesso: em 22 abr. 2020.

PREFEITURA DE JOINVILLE. **Instalada 1ª antena de rede de Internet das Coisas em Joinville**. Joinville. 23 ago. 2017. Disponível em: <https://www.joinville.sc.gov.br/noticias/instalada-1a-antena-de-rede-de-internet-das-coisas-em-joinville/>. Acesso em: 22 mar. 2020.

ROBL FILHO, Ilton Norberto. **Direito, Intimidade e Vida Privada**: Paradoxos jurídicos e sociais na sociedade hipermoderna. Curitiba: Juruá, 2008.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROSA, Alexandre Moraes da. A questão digital: o impacto da inteligência artificial no Direito. **Revista de Direito da Faculdade Guanambi**, Guanambi, v.6, n.2, p.1-18, 2018.

ROSA, Alexandre Moraes; VIEIRA, Marília Raposo. **Cloud Act: Quando a investigação se dá nas nuvens americanas**. 2019. Disponível em: <https://www.conjur.com.br/2019-nov-22/limite-penal-cloud-act-quando-investigacao-nuvens-americanas>. Acesso em: 9 abr. 2020.

ROSA, Luiz Pinguelli. **Introdução ao problema da Inteligência Artificial e da mente**. 2019. Disponível em: <https://cosmosecontexto.org.br/introducao-ao-problema-da-inteligencia-artificial-e-da-mente>. Acesso em: 8 mar. 2020.

RUARO, Regina Linden. Privacidade e autodeterminação informativa: obstáculos ao estado de vigilância? **Arquivo Jurídico**, Teresina – PI, v.2, n.1, p.41-60, Jan./Jun., 2015.

SANTOS, Fábio Marques Ferreira. **O limite cognitivo do poder humano judicante a um passo de um novo paradigma cognitivo de justiça**: poder cibernético judicante – o direito mediado por inteligência artificial. 668f. Tese (Doutorado). Pontifícia Universidade Católica de São Paulo, PUC-SP, 2016.

SANTOS, Gustavo Ferreira. **Neoconstitucionalismo, Poder Judiciário e Direitos Fundamentais**. Curitiba: Juruá Editora, 2011.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 11. ed. Porto Alegre: Livraria do Advogado, 2012.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. São Paulo: Revista dos Tribunais, 2014.

SCHMIDT, Eric; COHEN, Jared. **A nova era digital**: como será o futuro das pessoas, das nações e dos negócios. Tradução de Ana Beatriz Rodrigues e Rogério Durst. Rio de Janeiro: Intrínseca, 2013.

SEARLE, J.R. **O mistério da consciência**. Trad. André Yuji Pinheiro Uema e Vladimir Safatle. São Paulo: Paz e Terra, 1998.

SILVA, Alexandre Assunção. **Sigilo das Comunicações na Internet**. Curitiba: Juruá Editora, 2017.

SILVA, Edson Ferreira da. **Direito à intimidade**: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002. São Paulo: Juarez Soares, 2003.

SILVA, José. Afonso da. **Curso de direito constitucional positivo**. 41 ed. São Paulo: Malheiros, 2018.

SILVEIRA, Alessandra; FROUFE, Pedro. Do mercado interno à cidadania de direitos: a proteção de dados pessoais como a questão jusfundamental identitária dos nossos tempos. *Unio – EU Law Journal*, v.4, n.2, p.1-17, 2018.

SOLOVE, Daniel J; ROTENBERG, Marc; SCHWARTZ, Paul M. **Privacy, information, and technology**. New York: Aspen Publishers, 2006.

STATISTA. **Data storage supply and demand worldwide, from 2009 to 2020 (in exabytes)**. STATISTA. Disponível em: <https://www.statista.com/statistics/751749/worldwide-data-storage-capacity-and-demand/>. Acesso em: 22 mar. 2020.

STEINMETZ, Wilson. **Colisão de direitos fundamentais e princípio da proporcionalidade**. Porto Alegre: Livraria do Advogado, 2001.

STRECK, Lênio Luiz. Hermenêutica, Estado e Política: uma visão do papel da Constituição em países periféricos. In CADEMARTORI, Daniela Mesquita Leutchuk; GARCIA, Marcos Leite (org.). **Reflexões sobre Política e Direito**. Homenagem aos Professores Osvaldo Ferreira de Melo e Cesar Luiz Pasold. Florianópolis: Conceito Editorial, 2008, p.231-233.

TOMASEVICIUS FILHO, Eduardo. Marco Civil da Internet: uma lei sem conteúdo normativo. **Revista USP**, São Paulo, v.30, n. 86, p. 269-285, Apr., 2016.

VIEIRA, Oscar Vilhena. **Direitos fundamentais**: uma leitura da jurisprudência do STF. São Paulo Malheiros, 2016.