UNIVERSIDADE FEDERAL DE SANTA MARIA - UFSM
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS - CCSH
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
MESTRADO EM DIREITO

Wiliam Costodio Lima

O TRATAMENTO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA ENTRE UNIÃO EUROPEIA E BRASIL: O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO PARA A TUTELA DE DIREITOS FUNDAMENTAIS

Santa Maria - RS
2020

Wiliam Costodio Lima

O TRATAMENTO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA ENTRE UNIÃO EUROPEIA E BRASIL: O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO PARA A TUTELA DE DIREITOS FUNDAMENTAIS

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-graduação em Direito, na Área de Concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede: atores, fatores e processos na mundialização, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial à obtenção do título de **Mestre em Direito.**

Orientadora: Profª. Drª. Rosane Leal da Silva

Santa Maria - RS

2020

Lima, Wiliam Costodio
O TRATAMENTO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA ENTRE UNIÃO EUROPEIA E BRASIL: O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO PARA A TUTELA DE DIREITOS FUNDAMENTAIS / Wiliam Costodio Lima.- 2020.
106 p.; 30 cm

Orientadora: Rosane Leal da Silva
Dissertação (mestrado) - Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Direito, RS, 2020

1. Autoridade Nacional de Proteção de dados 2. Direitos fundamentais 3. Proteção de dados pessoais 4. Riscos I. Silva, Rosane Leal da II. Título.

Sistema de geração automática de ficha catalográfica da UFSM. Dados fornecidos pelo autor(a). Sob supervisão da Direção da Divisão de Processos Técnicos da Biblioteca Central. Bibliotecária responsável Paula Schoenfeldt Patta CRB 10/1728.

Declaro, WILIAM COSTODIO LIMA, para os devidos fins e sob as penas da lei, que a pesquisa constante neste trabalho de conclusão de curso (Dissertação) foi por mim elaborada e que as informações necessárias objeto de consulta em literatura e outras fontes estão devidamente referenciadas. Declaro, ainda, que este trabalho ou parte dele não foi apresentado anteriormente para obtenção de qualquer outro grau acadêmico, estando ciente de que a inveracidade da presente declaração poderá resultar na anulação da titulação pela Universidade, entre outras consequências legais.

Wiliam Costodio Lima

O TRATAMENTO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA ENTRE UNIÃO EUROPEIA E BRASIL: O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO PARA A TUTELA DE DIREITOS FUNDAMENTAIS

Dissertação apresentada ao Curso de Mestrado do Programa de Pós-graduação em Direito, na Área de Concentração Direitos Emergentes na Sociedade Global, com ênfase na Linha de Pesquisa Direitos na Sociedade em Rede: atores, fatores e processos na mundialização, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial à obtenção do título de **Mestre em Direito.**

Aprovado em 30 de março de 2020.

Rosane Leal da Silva, Dra. (UFSM)

Rafael Santos de Oliveira, Dr. (UFSM)

Vinícius Borges Fortes, PhD. (IMED)

Santa Maria - RS

2020

DEDICATÓRIA

À minha filha Bianca.

AGRADECIMENTOS

Agradeço a oportunidade de realizar o sonho de estudar na Universidade Federal de Santa Maria e obter o título de mestre em Direito.

Dedico este trabalho à minha filha Bianca. Não ousaria revelar aqui traços de minha intimidade diante da importância do tema tratado, de relevância para o desenvolvimento da personalidade e dignidade da pessoa humana. Seria um contrassenso. Contudo, devo registrar alguns pontos que considero importantes para a minha trajetória, como acadêmico e como pai. A contraprestação a estes estudos foi caríssima. Tempo e distância. Se posso sair hoje do ensino do mestrado, tudo foi graças a Bianca. Seu sorriso me faz enxergar que tudo vale a pena. Sou um cidadão que lutou no ensino público fundamental. Enfrento diariamente desafios da advocacia e da vida. Ser agraciado com o direito de estudar em uma universidade pública, federal, na minha cidade natal, é a construção simbólica que desejo que fique como inspiração a ela, e por um mundo melhor.

Agradeço minha mãe Inês, que esteve comigo nos momentos bons e ruins. É a pessoa que mais admiro neste mundo. À minha irmã Gabrielly, meu irmão Wedner, e meu pai Sérgio, pela força que me trouxeram até aqui.

À Escola Estadual de 1º e 2º grau Coronel Pillar, onde estudei o ensino fundamental e médio, graças ao esforço de professores e servidores públicos. Espero que tenha servido como exemplo de êxito do ensino público e da educação, ou ao menos, de uma pessoa humana.

À minha orientadora, Professora Rosane Leal da Silva, pela confiança depositada e seu incentivo. Obrigado pela orientação. Não existem palavras para agradecer. Em momentos difíceis, sempre aparece alguém para nos ajudar. Sempre confiei nisso. Agradeço à professora Rosane por ter me acompanhado e ajudado em um momento especial na minha vida.

Aos professores do Programa de Pós-Graduação em Direito da Universidade Federal de Santa Maria, em que tive a oportunidade de aproveitar cada minuto de aula. O conhecimento que obtive foi um sonho realizado. Especialmente, agradeço ao professor Rafael pela convivência oportunizada no grupo de pesquisa que preside o Centro de Pesquisas e Estudos em Direito e Internet (CEPEDI), cujo fiz parte por 03 (três) anos. Agradeço também pelas valiosas reflexões trazidas na banca de qualificação, assim como o fez o professor Vinícius Borges Fortes.

Aos amigos que fiz na UFSM, colegas e serventuários.

Aos familiares e amigos que me acompanharam nesta jornada, em especial ao Thiago, ao Dérico, a Bruna, e a todos os colegas de mestrado. Muito obrigado!

"[...] O judaísmo de Yonah viveria em sua alma, onde não podia ser molestado. Sempre, no entanto, que fosse seguro, ele iria até aquele aposento para visitar os objetos que havia lá. E, se sua vida fosse longa o bastante para ver os filhos atingirem a idade da razão, levaria cada um àquele lugar secreto.

Acenderia as velas, entoaria preces desconhecidas e tentaria ajudar a geração seguinte da família Callicó a compreender como era antes. Contaria as fábulas, as histórias de tios e avós que a criança nunca ia conhecer, falaria de magníficos objetos sagrados, de um homem cujas as mãos e cérebro tiravam maravilhas do metal e de uma rosa de ouro com caule de prata. Histórias de um tempo que fora melhor e de uma família que não existia mais, de um mundo que desaparecera. Depois disso, ele e Adriana concordavam, ficava tudo nas mãos de Deus." (GORDON, Noah. O último judeu – uma história de horror na Inquisição).

RESUMO

O TRATAMENTO DE DADOS PESSOAIS EM PERSPECTIVA COMPARADA ENTRE UNIÃO EUROPEIA E BRASIL: O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO PARA A TUTELA DE DIREITOS FUNDAMENTAIS

Autor: Wiliam Costodio Lima
Orientadora: Profa. Dra. Rosane Leal da Silva

A sociedade em rede é marcada pelo intenso uso das tecnologias da informação e comunicação (TIC). Este fluxo informacional gera uma significativa quantidade de dados pessoais e seu tratamento tem sido alvo de atenção normativa nos países tecnologicamente desenvolvidos, não no Brasil, desde a década de 70, tendo em vista os potenciais riscos desta dinâmica. Diante disto, este estudo tem como objetivo analisar criticamente os riscos aos direitos fundamentais derivados da utilização dos dados pessoais pelos Estados e pelo mercado para verificar e discutir o tratamento jurídico do tema em perspectiva comparada entre União Europeia e Brasil, examinando como estas legislações tratam da regulação dos fluxos informacionais e dos instrumentos delineados para a tutela dos dados, com ênfase para a atuação da Autoridade Nacional de Proteção de Dados. Tal investigação harmoniza-se com a linha de pesquisa Direitos na sociedade em rede: atores, fatores e processos na mundialização, do Programa de Pós-Graduação em Direito e, partindo desse cenário de fluxos informacionais visa-se a responder ao seguinte problema de pesquisa formulado: o recente marco regulatório editado no Brasil referente à proteção de dados pessoais e criação da Autoridade Nacional de Proteção de Dados (ANPD) permitirá que o país seja considerado com o mesmo nível de proteção normativa da União Europeia? O marco teórico do presente trabalho é composto por Antonio Enrique Pérez Luño e Danilo Doneda, e será utilizado o método de abordagem dedutivo, com o procedimento comparativo e técnicas de análise documental e pesquisa bibliográfica. Os resultados demonstraram que a atuação da Autoridade Nacional de Proteção de Dados no Brasil será determinante para que o país seja considerado em um nível aceitável para a proteção dos dados pessoais e assim contribua para o controle dos riscos advindos do seu tratamento e utilização pelos Estados e pelo mercado. As conclusões sugerem que o Brasil pode alcançar um nível compatível com o sistema europeu de proteção de dados considerado um dos mais avançados, tendo em vista as iniciativas no país de governança multisetorial na Internet, embora os riscos do tratamento de dados ainda devam continuar a existir devido às características globais da Internet e sua ambivalência. É recomendável a inserção da proteção de dados no seu rol de direitos fundamentais, bem como a garantia de uma autoridade de proteção para fiscalizar o cumprimento das normas relativas à matéria.

Palavras-chave: Autoridade Nacional de Proteção de dados. Direitos fundamentais. Proteção de dados pessoais. Riscos.

ABSTRACT

TREATMENT OF PERSONAL DATA AS A COMPARISON PERSPECTIVE BETWEEN THE EUROPEAN UNION AND BRAZIL: THE ROLE OF THE NATIONAL DATA PROTECTION AUTHORITY AS AN INSTRUMENT FOR ASSURANCE OF FUNDAMENTAL RIGHTS

Author: Wiliam Costodio Lima
Advisor: Profa. Dra. Rosane Leal da Silva

The network society is marked by the intense use of information and communication technologies (ICT). This informational flow generates a significant amount of personal data and its treatment has been the subject of normative attention in technologically developed countries, not in Brazil, since the 1970s, in view of the potential risks of this dynamic. In view of this, this study aims to critically analyze the risks to fundamental rights derived from the use of personal data by States and the market to verify and discuss the legal treatment of the topic in a comparative perspective between the European Union and Brazil, examining how these laws deal with regulation of informational flows and instruments designed for data protection, with emphasis on the work of the National Data Protection Authority. Such investigation is in harmony with the line of research Rights in the network society: actors, factors and processes in the globalization, of the Postgraduate Program in Law and, starting from this scenario of informational flows, the aim is to answer the following research problem formulated: will the recent regulatory framework issued in Brazil regarding the protection of personal data and the creation of the National Data Protection Authority (ANPD) allow the country to be considered with the same normative level of protection as the European Union? The theoretical framework of this work is composed by Antonio Enrique Pérez Luño and Danilo Doneda, and the deductive approach method is used, with the comparative procedure and techniques of document analysis and bibliographic research. The results showed that the performance of the National Data Protection Supervisor in Brazil will be decisive for the country to be considered at an acceptable level for the protection of personal data and thus contribute to the control of the risks arising from its processing and use by States and by the market. The findings suggest that Brazil may reach a level compatible with the European data protection system considered one of the most advanced for multisector internet governance initiatives, although the risks of data processing still exist due to the characteristics Internet and its ambivalence. It is recommended to include data protection in your list of fundamental rights, as well as the guarantee of a protection authority to monitor compliance with the rules related to the matter.

Keywords: National Data Protection Authority. Fundamental rights. Data protection. Risk.

SUMÁRIO

1. INTRODUÇÃO

A sociedade em rede é marcada pelo intenso uso das tecnologias da informação e comunicação (TIC), havendo necessidade de regulação e proteção dos dados pessoais, pois seu tratamento e seus efeitos afetam o desenvolvimento dos países, os direitos humanos e a democracia. Esta proteção jurídica é conferida devido às repercussões da informática, especialmente no que se refere aos bancos de dados.

O intenso fluxo informacional promete ser um grande motor de transformação. A Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), por exemplo, no ano de 2019, publicou um relatório sobre as TIC para o desenvolvimento sustentável e recomendações de políticas públicas que garantem direitos, em que anota crer que as novas tecnologias como a Internet das Coisas e a Inteligência Artificial (IA), podem, combinadas, contribuir diretamente para a missão da Agenda 2030 das Nações Unidas e os Objetivos de Desenvolvimento Sustentável.

No entanto, o relatório (UNESCO, 2019) declara que para enfrentar os desafios oriundos das TIC para a medição do desenvolvimento, os governos nacionais devem fomentar e promover soluções inovadoras alinhadas com os padrões internacionais de privacidade e proteção de dados. Ainda que reconheçam o papel das TIC para o desenvolvimento sustentável, a proteção e promoção de direitos humanos e a consolidação da democracia, o documento admite que elas podem gerar efeito contrário, realçando os riscos associados à segurança dos dados pessoais.

Portanto, ao lado destas inovações, abre-se a discussão sobre o melhor uso do tratamento de dados pessoais para a sociedade. Devido à sofisticação de suas técnicas e sua precisão através do grande volume de dados e informações, diversas discussões surgiram acerca do tema, principalmente após o escândalo *Cambridge Analytica*, nas eleições americanas de 2016, fato que se revelou o poder desses dados. A importância do tema determinou, no ano de 2016, a aprovação do Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679), e no Brasil, em 2018, de sua primeira lei geral de proteção de dados pessoais.

É neste sentido que a União Europeia tem avançado na produção normativa sobre a proteção dos dados pessoais, modelo bastante desenvolvido e que tem inspirado vários países (incluindo Argentina e Uruguai), além de estabelecer *standards* mínimos para que um país seja considerado com um nível adequado de proteção. Na busca pela inclusão entre os países que dispõem de leis de proteção, o Brasil recentemente começou a investir no seu marco regulatório para o tema, o que suscita o interesse em discutir essas previsões normativas em perspectiva

comparada, com ênfase sobre o papel a ser desenvolvido pela Autoridade Nacional de Proteção de Dados.

Deste modo, resta clara a relevância jurídica do tema proposto. Por atingir todos os setores da vida, a proteção de dados exige compreender e analisar os processos políticos, econômicos e sociais para incluir diferentes aspectos relativos aos marcos regulatórios e proteção a direitos a fim de garantir que as TIC não vulnerem importantes direitos fundamentais.

Neste viés, que o presente estudo tem como objetivo analisar criticamente os riscos aos direitos fundamentais derivados da utilização dos dados pessoais pelos Estados e pelo mercado para verificar e discutir o tratamento jurídico do tema em perspectiva comparada entre União Europeia e Brasil, examinando como estas legislações tratam da regulação dos fluxos informacionais e dos instrumentos delineados para a tutela dos dados, com ênfase para a atuação da Autoridade Nacional de Proteção de Dados. Pretende-se, assim, discutir o modelo de regulação delineado, suas potencialidades e limites para que o Brasil alcance um nível adequado de tratamento jurídico do tema.

Para tal, foi formulado o seguinte problema de pesquisa: considerando os elementos e características da sociedade em rede, marcadas pelo intenso uso das tecnologias da informação e comunicação (TIC) e pelos novos riscos derivados dos fluxos informacionais, é possível afirmar, em perspectiva comparada, que o recente marco regulatório editado no Brasil referente à proteção de dados pessoais e criação da Autoridade Nacional de Proteção de Dados (ANPD) permitirá que o país seja considerado com o mesmo nível normativo de proteção da União Europeia?

A abordagem utilizada escolhida foi a dedutiva, pois o tema exige uma compreensão interdisciplinar para buscar melhores soluções jurídicas aos desafios do desenvolvimento tecnológico, assim como um diálogo entre diversos atores e campos do conhecimento. Deste modo, parte-se de uma descrição geral sobre os fluxos informacionais e a sua utilização pelos Estados e mercado, gerando riscos aos direitos fundamentais, para especificamente apontar possíveis caminhos para o aperfeiçoamento do novo sistema de proteção de dados pessoais que se inicia no Brasil, com ênfase para a abordagem comparada com a União Europeia quanto ao papel da autoridade nacional.

O método de procedimento adotado foi o comparativo, devido à emergência destes novos instrumentos normativos aprovados pela União Europeia e pelo Brasil, de modo a constatar semelhanças e diferenças nos seus regimes jurídicos. Tendo em vista que o Brasil recentemente aprovou seu marco normativo, o estudo comparativo se mostra adequado para

projetar a atuação da autoridade nacional de proteção de dados no sistema de proteção de dados do país. As técnicas utilizadas foram análise de documentação indireta com pesquisa bibliográfica e documental (LAKATOS, 2003), diante da facilidade de acesso aos documentos que tratam da aprovação do recente instrumento normativo europeu e brasileiro de proteção de dados, o que permite analisar com maior profundidade o tema.

O presente estudo elegeu como marco teórico autores das ciências sociais e humanas que são a base para o desenvolvimento da investigação aqui proposta. A primeira parte terá como foco a dinâmica das condições sociais, econômicas e políticas e o consequente redimensionamento de direitos e novas formas de proteção de direitos fundamentais, com amparo nas obras de Antonio Pérez Luño, em que o autor trabalha a categoria de *cibercidadania*, reunindo um ponto de vista histórico dos direitos humanos com as consequências do desenvolvimento tecnológico.

O referido autor tem importantes contribuições sobre o direito e a Internet, especialmente ao tratar da passagem de concepções de superação do sujeito de direito vinculados ao Estado Liberal e Estado Social para a cidadania, adotando conceito ligado à democracia e o Estado de direito constitucional, ao que agrega ainda as transformações sociais, econômicas e políticas do desenvolvimento tecnológico. Faz-se necessário, assim, a regulamentação jurídica e a visão interdisciplinar diante das repercussões sócio políticas das tecnologias da informação e comunicação.

A segunda parte deste estudo, que tem como enfoque os instrumentos jurídicos decorrentes da utilização de banco de dados, teve como base teórica as reflexões de Danilo Doneda, autor que compreende a proteção de dados como um direito fundamental autônomo que precisa ser tutelado através de leis que garantam este "novo" direito e o desenvolvimento de formas inovadoras de tutela. Além disto, defende a existência de uma autoridade administrativa independente dedicada à proteção de dados pessoais representando a realização de uma garantia institucional.

Neste caminho, optou-se por dividir a dissertação em dois capítulos. No primeiro, a finalidade é discorrer criticamente sobre os novos riscos aos direitos fundamentais derivados do uso das TIC pelos Estados e pelo mercado, com ênfase para os dados pessoais vulnerados na sociedade em rede, sendo subdividido em duas partes. Em um primeiro momento, apresenta-se o conceito de *cibercidadania* para explorar os riscos das novas tecnologias cuja realidade remete a uma cibervigilância devido a utilização dos dados pessoais pelos Estados. Na segunda parte, explora-se a vulnerabilidade do indivíduo diante das tramas da rede e os dados pessoais em face do poder invisível do mercado. Já o segundo capítulo tem o enfoque normativo, onde

apresentam-se o tratamento jurídico dos dados pessoais, com ênfase para a atuação da autoridade nacional de proteção de dados em perspectiva comparada, sendo subdividido em duas partes. No primeiro subtítulo, é abordado o marco regulatório dos dados pessoais na União Europeia e o papel da autoridade nacional de proteção de dados. E no segundo subtítulo, busca-se discutir a trajetória brasileira na proteção de dados pessoais em perspectiva comparada, desde as promessas normativas para a atuação da autoridade nacional.

A temática possui relação com o Núcleo de Direito Informacional (NUDI), grupo vinculado ao Programa de Pós-Graduação em Direito da UFSM. Ademais, este estudo integra o projeto "O tratamento jurídico dos direitos fundamentais em tempos de Internet: diálogo entre direito interno e comparado" que objetiva, em suma, analisar os impactos que o desenvolvimento e utilização das tecnologias da informação e comunicação produzem sobre os direitos fundamentais e as respostas que a sociedade civil e o Estado têm oferecido.

Por fim, a pesquisa se vincula a área de concentração "Direitos Emergentes na Sociedade Global", especificamente a linha de pesquisa "Direitos na Sociedade em Rede: atores, fatores e processos na mundialização", eis que implica na observância de leis locais e globais e a participação de diversos atores para a preservação de direitos fundamentais decorrentes do uso das novas tecnologias. Outrossim, seu teor, profundidade e alcance convidam ao diálogo constante entre várias áreas do conhecimento, capazes de auxiliar no processo decisório de uma sociedade global, sempre levando em conta a análise crítica entre as exigências dos avanços tecnológicos e a proteção de direitos humanos e fundamentais.

2. OS FLUXOS INFORMACIONAIS NA SOCIEDADE EM REDE: novos riscos aos dados pessoais derivados do uso das TIC

O primeiro capítulo desta dissertação visará discorrer criticamente sobre os novos riscos aos direitos humanos e fundamentais[1] decorrentes das tecnologias da informação e comunicação, com ênfase para os dados pessoais vulnerados na sociedade em rede e sua utilização pelos Estados e pelo mercado. Ao se abordar estes riscos e suas repercussões jurídicos, políticas e sociais, visa-se uma compreensão mais aprofundada sobre o regime de proteção de dados que se inicia no Brasil e a criação de uma autoridade de proteção independente, de modo a enfatizar a necessidade de regulação e contribuir para o seu debate e aperfeiçoamento.

Desde o início, será possível observar que as terminologias *direitos humanos* e *direitos fundamentais* se entrelaçam quando se aborda a proteção de dados. A utilização massiva de dados pessoais por organismos estatais e privados com o desenvolvimento de tecnologias da informação e comunicação cada vez mais avançadas, representam novos desafios a estes. Estas categorias de direitos não significam a mesma coisa, por mais que exista uma profunda inter-relação entre ambas.

> Os direitos humanos possuem uma indissociável dimensão deontológica. Trata-se daquelas faculdades inerentes a pessoa que devem ser reconhecidas pelo direito positivo. Quando se produz esse reconhecimento aparecem os direitos fundamentais, cujo nome evoca sua função fundamentadora da ordem jurídica dos Estados de Direito (PÉREZ LUÑO, 2007, p. 105-106).

Ao se abordar os riscos aos direitos humanos decorrentes do tratamento dos dados pessoais pelos Estados e pelo mercado, almeja-se evidenciá-lo como um novo direito fundamental a ser regulado e tutelado. Tal abordagem aprofunda-se na medida em que o modelo europeu reconhece à proteção de dados como direito fundamental autônomo através de uma longa luta que se iniciou no direito humano à privacidade, enquanto no Brasil, busca-se o seu reconhecimento na Constituição Federal. As terminologias abordadas constantemente, portanto, não significam sinônimos, mas como nos termos acima enfatizados, se entrelaçam.

[1] Não se desconhece a existência de doutrinadores que se reportam aos direitos humanos e direitos fundamentais como sinônimos, como explica Sarlet (2015, p. 322).

2.1. Das promessas de *cibercidadania* à realidade da cibervigilância: os dados pessoais e sua utilização pelos Estados

O Estado deve tutelar os dados pessoais eis que seu tratamento gera riscos. Um dos primeiros conceitos legais sobre dados pessoais de relevância é observado na Convenção 108 do Conselho da Europa, de 1981 (seu tratamento jurídico é aprofundado no segundo capítulo), nos seguintes termos:

> **Artigo 1º - Objetivos e finalidades.** A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»). **Artigo 2º - Definições.** Para os fins da presente Convenção: **a)** «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados») [...]

Em razão disto, os dados pessoais, neste primeiro capítulo, são tratados em conjunto com o termo *informações*. Como se observa, diante do tratamento automatizado dos dados de caráter pessoal, é preciso garantir o respeito pelos direitos e liberdades fundamentais e o direito à vida privada. Para aprofundar o surgimento deste tratamento automatizado e o direito à proteção de dados que deste fenômeno decorre, antes oportuno refletir sobre as implicações do direito e as novas tecnologias.

Pérez Luño (2003) e sua visão geracional[2] e histórica sobre os direitos humanos e suas análises sobre a relação entre o direito e as novas tecnologias auxiliam o presente estudo servindo de ferramenta teórica para a compreensão do tema. A visão histórica dos direitos humanos permite considerar o contexto histórico do nascimento dos direitos. A relação entre o direito e as novas tecnologias aponta para novos riscos para os direitos humanos.

Há também de se rejeitar a ideia que muitas pessoas ainda têm de que os direitos humanos sempre existiram e não estão condicionados a determinadas lutas históricas. Os direitos humanos representam uma luta histórica vinculados ao seu tempo e seu contexto. Considerando a onipresença das novas tecnologias nas vidas das pessoas atualmente, certamente novos direitos e novas reivindicações surgem e direitos se modificam. O contexto histórico dos direitos humanos observa esta dinâmica e sua visão geracional permite didaticamente identificar novos riscos aos direitos humanos diante do desenvolvimento tecnológico.

[2] Há autores que preferem falar em dimensões dos direitos humanos, para não sugerir uma superação de uma geração de direitos sobre a outra, mas sim seu caráter de complementariedade (SARLET, 2015, p. 322).

Em um breve resumo, é possível descrever que a mutação histórica dos direitos humanos se inicia com a modernidade iluminista e a revolução burguesa do século XVII, com a primeira geração de direitos, considerados assim os direitos civis e políticos individuais, vinculados à liberdade, à igualdade, à propriedade, à segurança e à resistência às diversas formas de opressão (PÉREZ LUÑO, 2013, p. 167). Decorrem do pensamento liberal-burguês da época, marcado pelo cunho individualista, negativo e de oposição ao Estado (SARLET, 2015, p. 324).

Posteriormente, vieram os direitos de segunda geração, decorrentes das lutas sociais do século XIX e o impacto da industrialização, no sentido de completar os direitos de primeira geração, como os direitos econômicos, sociais, culturais (PÉREZ LUÑO, 2013, p. 167). A característica que distingue estes direitos para os de primeira geração, é que estes direitos demandam um comportamento ativo do Estado, assegurando ao indivíduo direitos a prestações sociais por sua parte (SARLET, 2015, p. 325).

Em complemento, observe-se a lição de Pérez Luño (2013, p. 167, tradução nossa.):

> Este contexto genético confere aos direitos humanos uns perfis ideológicos definidos. Os direitos humanos nascem, como é notório, com traço individualista, como liberdades individuais que configuram a primeira fase da geração de direitos humanos. Dita matriz ideológica individualista sofrerá um amplo processo de erosão e impugnação nas lutas sociais do século XIX. Estes movimentos reivindicativos evidenciaram a necessidade de completar o catálogo dos direitos e liberdades da primeira geração com a segunda geração de direitos: os direitos econômicos, sociais e culturais. Estes direitos alcançam sua palatina consagração jurídica e política e a substituição do Estado liberal pelo Estado social de Direito.

Destaca-se, assim, o caráter complementar dos direitos sociais de segunda geração em relação aos direitos de primeira geração. Veja-se que, no plano internacional, partindo-se da Declaração da Organizações das Nações Unidas de 1948, o reconhecimento de direitos civis e políticos ocorreu no mesmo ano do reconhecimento dos direitos sociais, econômicos e culturais, razão pela qual, são as principais características de cada geração, e não uma falsa impressão de substituição gradativa, que servem de auxílio para análises de natureza crítica.

Prosseguindo, Pérez Luño (2013, p. 168) afirma que atualmente tem se discutido estar-se em uma terceira geração de direitos humanos, em complementação as anteriores, através de estratégias reivindicativas em temas como o direito à paz, os direitos dos consumidores, os direitos decorrentes das biotecnologias e da manipulação genética, direito à qualidade de vida e à liberdade informática. Aqui, portanto, o encontro entre os direitos fundamentais e as novas tecnologias. Como afirma Sarlet (2015, p. 326), decorrem do "[...] impacto tecnológico, pelo estado crônico de beligerância, bem como pelo processo de descolonização do segundo pós-

guerra e suas contundentes consequências, acarretando profundos reflexos na esfera dos direitos fundamentais.”.

A terminologia “direitos humanos de terceira geração”, teria sido pronunciada por Karel Vasak, diretor jurídico da UNESCO, em 1979, em uma sessão internacional de direitos humanos, sustentando que seria necessária uma terceira geração de direitos, que complementariam as liberdades civis e políticas da primeira, com os direitos econômicos, sociais e culturais da segunda (PÉREZ LUÑO, 2013, p. 168.). Pérez Luño (2013, p. 168) ressalta que estas três gerações correspondem a evolução das três formas de Estado de direito e suas correlativas gerações de direitos, com as liberdades individuais representando o Estado liberal, os direitos econômicos, sociais e culturais constituindo o Estado social, e a terceira geração representando o modelo político atual do Estado Constitucional de direito. Desse modo, resta claro o caráter de complementariedade das gerações de direitos, no sentido de ampliação dos direitos liberais e sociais e a necessidade de solidariedade e solução pacífica de conflitos entre os povos de diferentes nações.

Contudo, existe uma polêmica acerca da existência de uma terceira geração de direitos humanos. Enfatiza-se, que os direitos já se encontram tutelados na primeira e segunda geração. Neste sentido, Pérez Luño destaca a *cibercidadania* como um novo horizonte dos direitos. Nas primeiras versões do Estado liberal, havia a exclusão das mulheres, crianças e adolescentes, analfabetos e indigentes do conceito de cidadania. Posteriormente, cidadania significava o desfrute de direitos sociais, econômicos e culturais, que também não eram estendidos a todos. Sua noção, portanto, passa por uma crise. O conceito de cidadania deve, então, ser aberto e discutido segundo as exigências políticas do presente (PÉREZ LUÑO, 2003).

Com as novas tecnologias se potencializam as possibilidades de participação direta do cidadão na esfera pública. Além disto, Pérez Luño (2003) observa que as garantias cívicas ganham maior exigência de que em qualquer outra etapa histórica, implicando em uma universalidade dos direitos das pessoas, para que se tutelem sem discriminação alguma por razões de raça, de língua, de sexo, das religiões e convicções ideológicas.

Em outro viés, Rodotà (2013) lembra que a comunicação televisiva, com sua característica vertical, acabava por ocasionar a personificação e a política simbólica, favorecendo sistemas populistas. Assim, uma das consequências foram o enfraquecimento dos sindicatos e a transformação dos partidos políticos, como forma de organização da sociedade para suas reinvindicações políticas, devido ao protagonismo da era televisiva. O desenvolvimento do marketing, a difusão do rádio, do telefone e da televisão tiveram como impacto o enfraquecimento da soberania popular e da cidadania.

As tecnologias da informação e comunicação, por sua vez, têm o potencial de oferecer maior informação[3], ampliando a cidadania antes reduzida. Com mais informação, é possível diminuir a discricionariedade administrativa, forçando a transparência e a democratização do sistema administrativo e favorecendo um controle cidadão da administração (RODOTÀ, 2013). O impacto da Internet no exercício das liberdades tem repercussões no âmbito da cidadania, e a este reforço dos direitos cívicos (e políticos) que Pérez Luño chama de *cibercidadania*, uma visão otimista das novas tecnologias (PÉREZ LUÑO, 2003).

Entretanto, assim como suas capacidades emancipatórias, as novas tecnologias não escapam seus riscos (PÉREZ LUÑO, 2013, p. 170). Pérez Luño (2002, p. 116-118) frisa que a Internet pode ser a principal ferramenta para promover uma participação política mais autêntica, plena e efetiva nas democracias do século XXI, o que se pode chamar de uma verdadeira *cibercidadania.* Porém, pode ser um fenômeno de controle da vida cívica, uma *cidadania.com,* como ilustra a literatura do lado perverso das novas tecnologias.

> A complexidade da vida moderna, as imensas possibilidades que nas grandes sociedades de nosso tempo se oferecem para deixar no anonimato ou na impunidade condutas antissociais ou delitivas exigem impor o funcionamento de meios de informação e controle. Porém estas observações não pretendem conduzir a falsa afirmação de que seriam inertes o Estado e a sociedade, e os cidadãos deveriam aceitar a existência de um colossal aparato informático e de controle, não se sabendo ao certo o nível de informação possuído, quem pode utilizar essas informações e com que finalidade irão fazê-lo. (PÉREZ LUÑO, 2003, p. 105, tradução nossa.).

Ao invés de uma promoção de direitos fundamentais concretizados pelo contexto atual da cidadania, as novas tecnologias os reduziriam. Estes riscos, segundo Pérez Luño (2003), podem ser classificados como jurídicos, sociais e políticos. Os riscos políticos seriam de uma verticalização da política, uma mercantilização da esfera pública e a apatia política. Os riscos morais apontam para uma carência da realidade e os riscos jurídicos para uma degradação do processo legislativo, um aumento da criminalidade informática e uma invasão da intimidade.

Veja-se que os riscos apontados por Pérez Luño decorrentes das novas tecnologias atingem direitos fundamentais individuais e coletivos, fator que marca os direitos de terceira geração. Estas análises teóricas sobre as gerações de direitos humanos e o nascimento da liberdade informática diante da realidade de riscos advindos das novas tecnologias encontram consonância com o debate conceitual da privacidade.

---

[3] Fala-se aqui no acesso à informação como empoderamento do cidadão frente ao Estado, mas não se pode negar que atualmente a disseminação de notícias falsas como práticas do mercado acabam por outro lado fragilizando os direitos dos cidadãos. Estas perspectivas do descontrole da informação e desinformação serão melhor exploradas no subcapítulo posterior.

O advento da informática e as mudanças políticas e sociais que lhe são correlatas constituem um ponto de inflexão para a ordem jurídica e seu primeiro desafio é compreendê-lo (DONEDA, 2006, p. 171). Por sua vez, o conceito de privacidade, se transforma, desde uma ótica individualista e de resistência à opressão psíquica e física, à uma óptica coletiva, diante da convergência de controle social aos dados pessoais.

Fala-se que a origem do direito à privacidade encontra-se no famoso artigo "The right to privacy" de Samuel Warren e Louis Brandeis, de 1890, nos EUA. O direito de privacidade, em sua concepção inicial, reflete a tendência a uma fundamentação diversa à desenvolvida pelo direito de propriedade que começa a despontar, e um dos seus pontos fundamentais é "[...] a observação, de que o princípio a ser observado na proteção à privacidade, no caso específico, na publicação de escritos pessoais, não passa pela propriedade privada, porém pela chamada *'inviolate personality'".* (DONEDA, 2006, p. 136). Para Leonardi (2011, p. 51), este era o propósito do artigo, e "[...] seu valor não está no direito de receber indenização em decorrência da publicação, mas sim na paz de espírito ou no alívio assegurado pela capacidade de impedir a própria publicação.".

O direito de ser deixado só inicia sua reivindicação jurídica diante do surgimento e desenvolvimento de jornais, revistas e fotografias, e a invasão em fatos que diziam respeito à vida privada das pessoas, com potencial dano à suas imagens, ainda que não restasse caracterizada a ocorrência de um crime de difamação ou calúnia, em que a honra já era objeto de proteção jurídica. Diante de novas formas potenciais de invasão da vida das pessoas, passou-se a preocupar-se com a tutela da vida privada, implicando na reivindicação de um novo direito, denominado como direito à privacidade.

Este artigo apresenta algumas características inéditas na proposição de um direito à privacidade. Primeiro, partindo de um fato social, que eram as mudanças advindas das novas tecnologias, como jornais e fotografias e a comunicação de massa. Em segundo, este direito seria de natureza pessoal e não se aproveitaria da proteção à propriedade para proteger a privacidade.

A reflexão sobre o artigo de Warren e Brandeis ainda hoje serve como ferramenta para a compreensão do nascimento deste novo direito. O direito de ser deixado só entende a privacidade como "[...] uma espécie de imunidade do indivíduo perante terceiros, um isolamento social, verdadeira *privação*." (LEONARDI, 2011, p. 54, grifo do autor), mas por outro lado, "[...] não nos permite determinar parâmetros para tutelar o que ela representa em um mundo no qual o fluxo de informações aumenta incessantemente, assim como aumenta o

número de oportunidades de realizarmos escolhas que podem influir na definição da nossa esfera privada.". (DONEDA, 2006, p. 01).

Em que pese as devidas ressalvas das diferenças entre o modelo anglo-saxônico e o romano-germânico, pode-se afirmar que a origem do direito à privacidade e sua constitucionalização advém do famoso artigo (MENDES, 2008, p. 15-16). O direito à privacidade passa a ser reconhecido internacionalmente na Declaração Americana de Direitos e Deveres do Homem[4], Declaração Universal dos Direitos do homem[5], Convenção Americana dos Direitos do Homem[6] e Convenção Europeia dos Direitos do Homem[7].

Veja-se que alguns dos dispositivos dizem respeito ao resguardo contra interferências alheias, como a inviolabilidade do domicílio e das correspondências, não sendo o equivalente ao isolamento, mas em ser deixado em paz para viver sua própria vida com um grau mínimo de interferência. No entanto, o conceito de privacidade não pode ficar restrito ao isolamento ou ao resguardo contra a interferência alheia, eis que "[...] nem todas as interferências alheias violam a privacidade, mas apenas aquelas relacionadas a dimensões específicas da pessoa, ou, a certas informações e assuntos peculiares.". (LEONARDI, 2011, p. 61).

No mesmo sentido, seria defini-lo como segredo ou sigilo, na divisão binária entre o público e o privado. Não há como viver em sociedade sem deixar um rastro de diversas informações, crescendo então a importância da ideia de privacidade como controle sobre a informação e os dados pessoais (LEONARDI, 2011).

Como se pode observar, o direito à intimidade e à privacidade consagrado nestes instrumentos jurídicos internacionais se relaciona com a liberdade e exigem uma abstenção do Estado. Em razão deste direito ter um caráter individualista, um "direito de ser deixado só" foi considerado por muito tempo um direito burguês. Ocorre que no decorrer do século XX, com a transformação do Estado juntamente com o surgimento das novas tecnologias, o direito à

---

[4] "Artigo 5º. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar. [...] Artigo 9º. Toda pessoa tem direito à inviolabilidade do seu domicílio. [...] "Artigo 10. Toda pessoa tem direito à inviolabilidade e circulação da sua correspondência.". (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1948).

[5] "Artigo 12 Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.". (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

[6] "Artigo 11. Proteção da honra e da dignidade. 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.". (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1969)

[7] "Artigo 8°. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.". (CONSELHO DA EUROPA, 1950).

privacidade muda seu sentido e alcance, passando a ser considerado como pressuposto para o reconhecimento de outros direitos fundamentais.

Assim, o direito à privacidade deixa de ser um problema das grandes celebridades para atingir a maioria dos cidadãos. A partir do tratamento informatizado dos dados, com sua rapidez e eficiência, novos desafios ao ordenamento jurídico surgem, ensejando o nascimento da disciplina de proteção de dados pessoais, associando a proteção à privacidade e informações pessoais.

> A partir da evolução da tecnologia da informação e das transformações do ordenamento jurídico, a privacidade deixa de ser concebida como o direito do indivíduo a ser deixado só, adquirindo progressivamente um caráter mais positivo, como sendo o direito de se construir uma esfera privada própria, a partir da idéia de livre desenvolvimento da personalidade. (MENDES, 2008, p. 10).

Deste modo, a proteção de dados pessoais passa a ser compreendida como um fenômeno coletivo, pois os potenciais danos causados pelo processamento de dados pessoais são de natureza difusa. Por consequência, a tutela jurídica deve ser coletiva. Além disto, a proteção de dados pessoais envolve o problema da igualdade, uma vez que o seu processamento gera sistemas de classificação e de risco. Conforme Leonardi (2011, p. 67), “Para essa corrente, a privacidade é a reinvindicação de indivíduos, grupos ou instituições, de determinar por si próprios quando, como e em que extensão informações a seu respeito são comunicadas a terceiros na conhecida definição de Alan Westin.”.

Tal interpretação decorre do fato de que a privacidade se constitui em um espaço de livre desenvolvimento do indivíduo. O titular do direito à privacidade tem autonomia para exercê-lo, nos termos da dignidade humana e no princípio da autodeterminação, que acabam se relacionando e se integrando com os demais direitos fundamentais (MENDES, 2008, p. 21). Este seria um dos conceitos mais influentes a respeito da privacidade (LEONARDI, 2011).

No entanto, a indefinição do conceito de privacidade é uma característica intrínseca da matéria, e “[...] a insistência em isolar as características essenciais da privacidade, e reuni-las em um conceito unitário, aplicável indefinidamente em qualquer situação, é tarefa que tende a ser fracassada.”. (LEONARDI, 2011, p. 51). Doneda (2006) ressalta que o exercício de conceituar a privacidade é puramente acadêmico, e estão ligados aos valores e projeções do homem em cada sociedade, refletindo um forte conteúdo social e ideológico.

O debate sobre o conceito de privacidade revela suas múltiplas faces, pois não somente funde-se entre um direito de caráter individualista e a capacidade de dispor de suas informações como bem entender, mas como também, em uma perspectiva americana, um conjunto de

direitos contra uma pluralidade de problemas distintos e relacionados entre si (LEONARDI, p.83). Nesta óptica, Pérez Luño (2003) ao discorrer sobre a *cidadania.com,* como um conjunto de riscos aos direitos fundamentais decorrentes do desenvolvimento tecnológico, possui muitos pontos em comum com este conceito plural de privacidade.

A liberdade informática, destaca as possibilidades de vigilância e classificação e controle social do desenvolvimento tecnológico, que teve como resposta jurídica a criação de instrumentos nacionais e internacionais, como a Convenção de Estrasburgo, de 1981, que como visto no início do presente subcapítulo, garante o respeito aos direitos e liberdades fundamentais, e especialmente ao direito à vida privada, face o tratamento automatizado de dados pessoais. Rodotà (2008) destaca que esta seria uma "utopia necessária", diante da realidade dos riscos gerados pelas condições de vigilância em nome da segurança e da lógica do mercado.

A fim de não exaurir o difícil debate conceitual da privacidade, e procurando efetivar o objetivo geral e específico de discorrer sobre os riscos aos direitos humanos e fundamentais decorrentes da utilização dos dados pessoais pelos Estados e pelo mercado na sociedade em rede, opta-se por uma interdisciplinaridade, de modo a enfatizar as consequências sociais e políticas do tratamento de dados. Pois, somente através de várias ópticas este fenômeno pode ser captado (PÉREZ LUÑO, 2003, p. 99).

O progresso tecnológico e a expansão de seus riscos, dizem respeito a questão de segurança interna e internacional e do funcionamento do mercado e a organização das empresas, das mídias, da globalização e da relação entre tecnologia, política e cidadania (RODOTA, 2008, p. 233). Nas palavras de Rodotá (2008, p. 233), "Apesar de acreditarmos estar apenas tratando do tema da proteção de dados, na verdade, estamos nos ocupando do destino das nossas sociedades, do seu presente e sobretudo do seu futuro.".

Deste modo, tem-se um ponto de encontro entre a liberdade informática, os conceitos de privacidade e as implicações para a teoria do estado (políticas) e do controle social (sociais) diante do desenvolvimento tecnológico. Ainda, é possível observar dos exemplos atuais de vigilância do Estado e do mercado que os riscos que culminaram na elaboração das primeiras leis de proteção de dados se expandiram de modo impressionante, justificando ainda mais a importância deste direito. Resume Doneda (2006, p. 181):

> Os dados pessoais passam a ser os intermediários entre a pessoa e a sociedade, prepostos nem sempre autorizados e capazes, e é justamente isto que produz como efeito a perda de controle da pessoa sobre o que se sabe em relação a si mesma – o que, em última análise, representa uma diminuição na sua própria liberdade.

Foi o Estado, o primeiro a perceber capaz de utilizar largamente as informações pessoais, o que implica em grande controle (DONEDA, 2006). A ampliação da capacidade de vigilância e controle social do Estado acaba por atingir direitos humanos e fundamentais como a liberdade, a dignidade da pessoa humana e a igualdade. Quanto mais segurança, menos liberdade. Veja-se que Giddens (1991, p. 12-13) aponta que uma das dimensões institucionais que caracterizam atualmente o que ele chama de sociedade de risco[8], é a existência do Estado-nação, em sua capacidade administrativa e o desenvolvimento de condições de vigilância muito superior em relação às civilizações tradicionais.

Foucault (2013), em seus escritos, já alertava sobre as "sociedades disciplinares" do século XIX como característica fundamental da criação do Estado-nação. As sociedades disciplinares vieram para substituir as monarquias soberanas, multiplicando-se por todo o corpo social as instituições de disciplina, tais como as oficinas, fábricas, escolas e prisões. Predominavam, assim, os modelos pan-ópticos de poder nas suas instituições com seus respetivos objetivos.

> A modalidade panóptica do poder – no nível elementar, técnico, humildemente físico em que se situa – não está na dependência imediata nem no prolongamento direto das grandes estruturas jurídico-políticas de uma sociedade; ela não é entretanto absolutamente independente. Historicamente, o processo pelo qual a burguesia se tornou no decorrer do século XVIII a classe politicamente dominante, abrigou-se atrás da instalação de um quadro jurídico explícito, codificado, formalmente igualitário, e através da organização de um regime de tipo parlamentar e representativo. Mas o desenvolvimento e a generalização dos dispositivos disciplinares constituíram a outra vertente, obscura, desse processo. A forma jurídica geral que garantia um sistema de direitos em princípio igualitários era sustentada por esses mecanismos miúdos, cotidianos e físicos, por todos esses sistemas de micropoder essencialmente inigualitários e assimétricos que constituem as disciplinas. E se, de uma maneira formal, o regime representativo permite que direta ou indiretamente, com ou sem revezamento, a vontade de todos forme a instância fundamental da soberania, as disciplinas dão, na base, garantia da submissão das forças e dos corpos. As disciplinas reais e corporais constituíram o subsolo das liberdades formais e jurídicas. (FOUCAULT, 2013, p. 209)

A vigilância sobre os corpos visava a obter informações e dados que permitissem separar as pessoas nos hospitais conforme suas enfermidades, para que não se espalhassem doenças. Informações pessoais também eram relevantes nas escolas para classificar os alunos conforme nível de conhecimento, de forma a direcionar para as funções correspondentes na divisão social

[8] As teorias da sociedade de risco (BECK, 2011; GIDDENS, 1991) têm posto em evidência que a sociedade contemporânea é marcada profundamente pelo progresso tecnológico e expansão de seus riscos. Trata-se, pois, de "[...] uma fase do desenvolvimento da sociedade moderna, em que os riscos sociais, políticos, econômicos e individuais tendem cada vez mais a escapar das instituições para o controle e a proteção da sociedade industrial.". (BECK, GIDDENS, LASH, 1997, p. 15).

do trabalho. Nas penitenciárias era igualmente vital classificar os presos conforme os graus de periculosidade, bem como na caserna, treinar as tropas e a obediência hierárquica. Tratava-se, portanto, de uma vigilância que limitava a liberdade física e psíquica das pessoas.

Antes do Estado moderno, não se podia falar em privacidade, diante das sociedades feudais e seus regimes de escravidão. Segundo Doneda (2006, p. 08), "Não havia realmente lugar para a tutela jurídica da privacidade em sociedades que confiavam sua regulação a outros mecanismos – fossem estes a rigidez da hierarquia social ou então a própria arquitetura dos espaços públicos e privados.".

O controle social visto através das instituições, também poderia ser observado da própria arquitetura das cidades. Em sua lógica militar, as condições que facultaram o nascimento das grandes cidades são as mesmas que tornam importantes os pontos estratégicos, uma arquitetura ligada ao poder político do Estado, e

> [...] em todo o lugar onde essas condições foram preenchidas, há centros populacionais; onde há circulação, há aglomeração urbana. [...] a ascensão do totalitarismo é perfeitamente equiparável ao desenvolvimento do controle estatal sobre a circulação das massas, e, portanto, desde a origem, facilmente identificável na história dos grandes organismos administrativos do Estado. (VIRILIO, 1996b, p. 26-29).

Esta obsessão pelo controle e pela informação no Estado moderno chega ao seu ápice de desenvolvimento nos regimes totalitários[9], durante a segunda guerra mundial, como bem desenvolveu Agamben (2002) analisando os campos de concentração nazistas. O autor comenta que Foucault, após estudar a história da sexualidade e suas implicações com o poder, começa a pesquisar a biopolítica nas prisões e nos hospitais, por exemplo, pois se constata "[...] a crescente implicação da vida natural do homem nos mecanismos e nos cálculos de poder [...]" (AGAMBEN, 2002, p. 123), mas deixa de fazê-lo nos campos de concentração.

Sendo o controle social ligado à soberania nacional, ou seja, uma ideia ligada a segurança interna e internacional, o cidadão passa a ser uma questão política essencial, pois tem que se definir quem é e quem não é "cidadão" (AGAMBEN, 2002, p. 135). Agamben (2002) reflete sobre os direitos que não tinham aqueles que não pertenciam ao Estado-nação, como os

[9] Para Agamben (2004, p. 13) "A contiguidade entre democracia de massa e Estados totalitários não tem, contudo (como Löwith parece aqui considerar, seguindo a trilha de Schmitt), a forma de uma improvisada reviravolta: antes de emergir impetuosamente à luz do nosso século [século XX], o rio da biopolítica, que arrasta consigo a vida do *homo sacer*, corre de modo subterrâneo, mas contínuo. É como se, a partir de um certo ponto, todo evento político decisivo tivesse sempre uma dupla face: os espaços, as liberdades e os direitos que os indivíduos adquirem no seu conflito com os poderes centrais simultaneamente preparam, a cada vez, uma tácita porém crescente inscrição de suas vidas na ordem estatal, oferecendo assim uma nova e mais temível instância ao poder soberano do qual desejariam liberar-se."

estrangeiros, e na medida em que os direitos do homem passam a ser ligado ao seu pertencimento, ser cidadão passa a ser seu novo fundamento. Em outras palavras, a crise do Estado moderno durante os estados totalitários do fascismo e do nazismo, onde "[...] a tutela da vida coincide com a luta contra o inimigo [...]" (AGAMBEN, 2002, p. 154), o campo e suas condições desumanas é resultado de uma estrutura político-jurídica[10].

A busca incessante pela informação para fins da política do Estado é a característica marcante do totalitarismo. Esta necessidade decorreu da definição daqueles que possuíam direitos, os cidadãos, para aqueles que não possuíam, como o estrangeiro (posteriormente, vieram leis de desnaturalização, mas é a constatação de Agamben da categorização pelo Estado que importa neste momento), tendo repercussões na sua capacidade de controle social.

Esta transformação das sociedades disciplinares, vindo em substituição àquelas desenvolvidas por Foucault através da família, escola, hospital, fábrica e prisão, como modelos que sucederam a sociedade de soberania, também se modificam no que diz respeito à segurança internacional em relação não apenas ao cidadão, mas também com os outros Estados. O fato marca a mudança da vigilância psíquica para a vigilância de dados pessoais e a transformação de um direito individualista de privacidade para a necessidade de extensão deste direito nas sociedades pós-industriais.

Virilio (2005) aponta que ao lado dos meios de comunicação como um tradicional serviço do controle social encarregado de garantir a propaganda dirigida às populações civis durante a primeira e segunda guerra mundial na primeira metade do século XX, como um serviço cinematográfico de propaganda, desenvolveu-se a necessidade de um serviço militar das imagens, visando garantir representações táticas e estratégicas dos conflitos (VIRILIO, 2005, p. 136). Tal vigilância altera sensivelmente o controle social atingindo direitos e liberdades das pessoas.

Desenvolvida durante a primeira guerra através do reconhecimento por balões (bidimensional), esta nova forma de vigilância fez com que alguns Estados, como a Grã-Bretanha, abandonassem os meios de defesa tradicionais, para dedicar-se à pesquisa da percepção, onde inicia-se a cibernética, o radar, o rádio e as telecomunicações (VIRILIO, 2005, p. 119). Em suma, o "[...] registro das câmeras ao longo do primeiro conflito mundial prefigurava a memória estatística dos computadores, tanto pela gestão dos dados fornecidos

[10] Na obra "Estado de Exceção" (2004), Agamben explica este conceito: "O totalitarismo moderno pode ser definido, nesse sentido, como a instauração, por meio do Estado de Exceção, de uma **Guerra Civil legal** que permite a eliminação física não só dos adversários políticos, mas também de categorias inteiras de cidadãos que, por qualquer razão, pareçam não integráveis ao sistema político.". (2004, p. 13, grifo nosso.).

pelo reconhecimento aéreo quanto pela simulação cada vez mais rigorosa da simultaneidade da ação e da reação.". (VIRILIO, 2005, p. 171).

O registro das câmeras fez-se desenvolver meios de comunicação para a transmissão mais rápida das mensagens como parte das estratégias dos grandes conflitos militares do século XX, em uma lógica de militarização para industrialização das tecnologias da informação e comunicação. Virilio (2005) alerta que ao se privilegiar este aparato de vigilância nas sociedades contemporâneas, os recursos tecnológicos cada vez mais irão estocar e manipular estas informações, sendo aí onde cresce a importância do controle e segurança de guarda e de sua transmissão.

O processamento através de computadores e câmeras de registro[11], evoluem até a bomba atômica e a guerra fria, obrigando os EUA a desenvolverem ainda mais a espionagem, através do infra-vermelho, termografia e centros de vigilância eletrônica, que através de computadores classificam automaticamente os dados transmitidos (VIRILIO, 2005, p. 190). Os efeitos eletrônicos, por volta de 1970, tornaram a guerra em uma "guerra híbrida", ou seja, "[...] o mundo desaparece na guerra e a guerra enquanto fenômeno desaparece aos olhos do mundo.". (VIRILIO, 2005, p. 161). Redes de televisão com transmissões ao vivo e ininterruptas, comercialização extraordinária de técnicas audiovisuais, como walkmans, são consequências desta expansão de técnicas militares na economia e na sociedade civil.

A partir deste desenvolvimento e transformação da vigilância decorrente dos conflitos militares, tem-se também uma nova perspectiva de controle social interno. Foucault (2008) ao refletir a mudança de paradigma na "arte de governar" dos Estados com o fim da segunda guerra mundial em meio ao século XX sinaliza que a legitimação jurídica do Estado-nação passa a se dar pelo consenso do crescimento econômico e adesão global da população ao regime e ao sistema, no que chamou de neoliberalismo. O Estado, para governar em uma economia de mercado, passa a adotar um liberalismo intervencionista, através de estabelecimento de monopólios, ações econômicas e políticas sociais (FOUCAULT, 2008, p. 185).

Nesse período que surgem as discussões sobre grandes bancos de dados estatais, como a *Natural Datacenter*, nos EUA, e o Sistema automatizado para o fichamento administrativo e o repertório dos indivíduos (SAFARI) na França (DONEDA, 2006). Estes debates ensejaram a reação da população e influenciou na aprovação das primeiras leis de proteção de dados, tanto nos EUA como na Europa.

[11] "A câmera reproduz as circunstâncias da visão comum, ela é testemunha homogênea da ação e, ainda que as imagens impliquem um retardamento, sua força consiste em dar ao espectador uma ilusão de proximidade em um conjunto temporal coerente.". (VIRILIO, 2005, p. 163).

Foucault (2008) explica que a teoria do Estado, na prática, está limitada ao mercantilismo, ao estado de polícia e a política internacional (diplomacia e forçar armadas). A limitação de sua atuação se dá através da economia política, esse modo de governar o bastante, de estabelecer verdades. O liberalismo, então, representa uma nova arte de governar, ainda no século XVIII, tendo sua razão em numerosas e complexas causas visando, sobretudo, assegurar o crescimento, mas também limitar do interior o exercício do poder de governar. Suas características são a constituição do mercado como lugar de formação da verdade e o problema da limitação do exercício do poder público através dos direitos do cidadão frente ao soberano. Em síntese, "[...] é um jogo complexo entre direitos fundamentais e independência dos governados. O governo, em todo o caso o governa na razão governamental, é algo que lhe manipula interesses.". (FOUCAULT, 2008, p. 61).

Resgatando o objetivo de discorrer sobre os riscos aos direitos fundamentais decorrentes da utilização dos dados pessoais pelos Estados, especificamente os sócio-políticos devido às políticas de segurança interna e internacional, a governamentalidade e toda a obra de Foucault, parafraseando Lafontaine (2007, p. 100-101), "[...] não deixa de ser atravessada pelo espírito do tempo.". Apesar de menções geralmente ao pan-ópticos na forma eletrônica, o biopoder e a governamentalidade, associado a ideia de Estado que viabiliza o desenvolvimento do capitalismo, é um dos conceitos da obra de Foucault determinantes na teoria do Estado, "[...] através do controle matemático dos corpos, dos fenômenos populacionais, da produção e dos processos econômicos.". (MENEZES NETO, 2016, p. 183).

Posteriormente, como será analisado, este biopoder se transforma em híbrido e necessita de modificações, pois os fluxos informacionais passam a ser globalizados e virtualizados. Mas, desde já se pode afirmar que se vive em uma sociedade pós-panóptica, onde departamentos do Estado e empresas privadas atuam, entre outras coisas, no sentido de observarem seus consumidores e assim auxiliarem na vigilância em massa global (MENEZES NETO, 2016, p. 118). Por isso, a observação do nascimento desta conjuntura que irá se expandir ao longo dos anos auxilia na compreensão de uma complexa forma de vigilância por meio as novas tecnologias e da utilização e tratamento dos dados pessoais.

Se uma das precauções relativas à privacidade é devido ao aumento do controle social, a transformação do modelo de vigilância do Estado revela sua predisposição por registrar e tomar conhecimento sobre todos os aspectos da vida das pessoas. Veja-se que para Foucault é impossível vigiar a totalidade do processo econômico. Ao apresentar o conceito de *homo oeconomicus,* que se caracteriza pelo cruzamento entre um sujeito de interesse e análises econômicas, permite-se desvendar o controle social pelo Estado a partir do mercado. Em sua

consistência moderna, o liberalismo começou "[...] quando precisamente, foi formulado essa incompatibilidade essencial entre, por um lado, a multiplicidade não totalizável do sujeito de interesse, dos sujeitos econômicos e, por outro lado, a unidade totalizante do soberano jurídico.". (FOUCAULT, 2008, p. 384). O *homo oeconomicus* e a sociedade civil fazem parte, portanto, do conjunto da "[...] tecnologia da governamentalidade liberal.". (FOUCAULT, 2008, p. 403).

O poder é um campo de relações e deve ser analisado por inteiro, pois a governamentalidade passa a agir sobre campos não econômicos como no caso da condução dos loucos, dos doentes, delinquentes e crianças (FOUCALT, 2008, p. 258). Se o modelo pan-óptico de Bentham influencia o projeto de modernidade diante do controle dos corpos individuais, os sistemas de tecnologia partem para o controle do corpo população e o Estado passa a não somente regular os atos econômicos do sujeito como seus atos não propriamente econômicos como o casamento e os filhos, mais posteriormente, o próprio patrimônio genético do sujeito[12].

Esta simbiose entre controle social para controle de segurança interna e internacional e o mercado, vai alavancar o seu desenvolvimento em direção a uma sociedade de controle, como bem observou Deleuze (1992). E a Internet será a tecnologia que culminará na ferramenta para controle social interno e internacional, ampliando os poderes de vigilância do Estado e limitando ainda mais a liberdade das pessoas.

A ameaça à privacidade constitui-se potencial redução da liberdade. De outro lado, a soberania do Estado é exercida através do controle da informação. Com o desenvolvimento da Internet, e seu caráter global, tem-se um novo espaço de vigilância e controle (CASTELLS, 2003, p. 150). Como afirma Pérez Luño (2002), se antes, os Estados para vigiar as comunicações tinham que violar correspondências, com a Internet se amplia imensuravelmente a capacidade de interceptação. Para Virilio (1997), a Internet e a globalização sinalizam o grande confinamento que Foucault observava no século XVIII nas "sociedades disciplinares", agora caracterizado pela ausência de espaço geográfico e tempo para comunicar-se, acabando por restringir a liberdade de movimento.

[12] "De fato, a genética atual mostra muito bem que um número de elementos muito mais considerável do que se podia imaginar até hoje [é] condicionado pelo equipamento genético que recebemos dos nossos ascendentes. Ela possibilita, em particular, estabelecer para um indivíduo dado, qualquer que seja ele, as probabilidades de contrair este ou aquele tipo de doença, numa idade dada, num período dado da vida ou de uma maneira totalmente banal num momento qualquer da vida. Em outras palavras, um dos interesses atuais da aplicação da genética às populações humanas é possibilitar reconhecer os indivíduos de risco e o tipo de risco que os indivíduos correm ao longo de sua existência. [...] esses bons equipamentos genéticos vão se tornar certamente uma coisa rara, e na medida em que será uma coisa rara poderão perfeitamente [entrar], e será perfeitamente normal que entrem, em circuitos ou em cálculos econômicos, isto é, em opções alternativas. (FOUCAULT, 2008, p. 313).

Agamben (2013) anota que, tem prevalecido sempre o conceito de segurança em detrimento de qualquer outra noção política, tendo-se assim um estado de exceção de violação de direitos individuais, com a convergência paradoxal de um paradigma de economia liberal com um paradigma de controle estatal e policial absoluto. Lafontaine (2007, p. 130), sustenta que a "[...] Internet e as novas tecnologias da informação estão estreitamente ligadas ao triunfo da economia de mercado à escala planetária. Sem partilharem necessariamente os valores neoliberais, os apologistas do ciberespaço mostram ser ardentes defensores da mundialização.". O mercado, como uma maneira de governar, acaba por definir esta exigência de vigilância das informações, o que consagra então a sociedade de controle, ou, na visão de Virilio (1997), uma sociedade cibernética, eis que se trata de um modelo autorregulado e não de liberdade e democracia[13].

> Graças à implementação paciente de uma interatividade estendida a todo o nosso planeta, a "guerra informática" prepara a primeira guerra mundial de tempo, ou mais precisamente: a primeira guerra de tempo mundial, desse "tempo real" de trocas redes interconectadas. É fácil ver que a atual globalização do mercado também tem três dimensões: geofísica, técnico-científica e ideológica, daí a inevitável aproximação entre o desejo dos Estados Unidos de generalizar o livre comércio global para o horizonte 2010-2020 e a preparação de uma guerra informática. Há uma impossibilidade de distinguir a guerra econômica da informática, já que é a mesma ambição hegemônica de tornar interativa a ideologia comercial e militar. (VIRILIO, 1998, p. 158, tradução nossa.).

Deste modo, se percebe como as novas tecnologias e os controles estatais limitam injustificadamente a liberdade. Através do funcionamento do mercado e da globalização, das mídias e alterando as assimetrias de poder entre o cidadão e o Estado, os riscos sócio-políticos são assim expandidos. E esta simbiose entre a ampliação dos poderes do Estado e do mercado, é uma das preocupações da privacidade e do tratamento de dados pessoais, e não uma substituição de vigilância de uma pela outra.

Como exemplo, tem-se os drones, uma das principais tecnologias de vigilância, cujo a capacidade de gerar informações se expande de modo impressionante (BAUMAN, 2014). A economia política da velocidade, de que fala Virilio (1997), seria uma maneira de conter os riscos de controle social das novas tecnologias, atuando de modo semelhante a economia

[13] "[...] Sistema, complexidade e auto-organização, outros tantos conceitos suportados pela segunda cibernética e que nos levam à convergência contemporânea entre o neoliberalismo e o paradigma informacional. Esta convergência passa, antes de mais e acima de tudo, pelo desenvolvimento das novas tecnologias da informação, mas também pela difusão de uma visão de mundo centrada na adaptabilidade. O relativismo pós-moderno constitui [...] um dos principais compostos intelectuais em que se desenvolve o paradigma informacional.". (LAFONTAINE, 2007, p. 158)

política da riqueza, que procura limitar a acumulação de capital, pois a Internet provoca ameaças à liberdade das pessoas.

Um dos componentes que fomentam a necessidade de vigilância e a implantação deste aparato estatal de controle social é o funcionamento da mídia. A mídia, primeiramente, configura o poder do Estado, sendo um instrumento de sua propaganda. Deste modo, o aumento do controle social por sua parte irá decorrer desta prevalência de comunicações simbólicas. Seu funcionamento é um elo entre as relações entre o Estado, a cidadania e as novas tecnologias.

A invasão estatal cada vez mais agressiva na esfera da intimidade das pessoas é efeito imediato de uma construção simbólica favorável nos espaços públicos. O efeito é estender os poderes repressivos do Estado em nome da segurança e convencer as pessoas que a invasão na sua intimidade serve para proporcionar mais a sua segurança e protegê-lo, quando na verdade o agride na sua esfera íntima, na liberdade e em sua dignidade. Por fim, o cidadão no espaço público tende a cair nas tramas da rede, contribuindo espontaneamente para a sua espionagem.

Castells (2009, p. 44) observa que o monopólio da violência pelo Estado configura seu poder social, que por sua vez depende da construção simbólica que em grande parte são criados e formados nas redes de comunicação na esfera pública. O autor lembra a capacidade de enquadrar a mente humana e as relações entre a política, cognição e emoção na tomada de decisões, como por exemplo, ocorreu com o público norte-americano no processo que levou à guerra do Iraque (CASTELLS, 2009, p. 207-208 e 232). Não restam dúvidas assim, da relação da comunicação e o controle social, e no caso específico, "[...] investigadores descobriram que as ligações cognitivas e as emocionais entre o terrorismo e a guerra do Iraque são decisivas no momento de aumentar os níveis de apoio à guerra.". (CASTELLS, 2009, p. 235).

Para Virilio (1997), o desenvolvimento da bomba atômica fez com que se desenvolvesse a bomba informática, ou mais precisamente, a bomba da informação totalitária. O autor recorda que o controle social era encarregado de garantir a propaganda dirigida às populações civis no cinema, tanto a serviço de Hitler, como também no "New Deal" de Roosevelt e a "guerra do mercado doméstico". A invenção da fotografia e depois das filmagens, desenvolvida na segunda guerra mundial, possibilitou estabelecer uma guerra ideológica através de propaganda no rádio e no cinema, com o objetivo de exercer o controle emocional das pessoas (VIRILIO, 2005).

Este paradoxo de economia liberal de mercado e aumento insaciável do Estado pelo controle se deve muito a este controle emocional desenvolvido nos espaços públicos como a mídia. Mas, há outros fatores, que em concomitância contribuem para um aumento da vigilância convergindo para os dados pessoais. O funcionamento da mídia, que engloba o mercado e a globalização, o que será também observado no subcapítulo seguinte, mas com o foco na

utilização dos dados pessoais pelo mercado, contribui para uma vigilância estatal. Nas mídias sociais, por exemplo, a morte do anonimato se dá por vontade própria, o que demonstra a correção das análises de que a privacidade engloba uma série de situações distintas e entrelaçadas entre si, que exige uma abordagem interdisciplinar tendo em vista a complexa relação jurídica que disto resulta.

> [...] com o Facebook, dá para ver o comportamento dos usuários, que ficam felizes em divulgar qualquer tipo de dado pessoal, e será que é justo culpa-los por não saber qual é o limite entre privacidade e publicidade? Alguns anos atrás, antes das tecnologias digitais, as pessoas famosas eram as celebridades, os políticos ou os jornalistas, mas hoje qualquer pessoa tem potencial para a vida pública, basta clicar no botão "publicar". "Publicar" significa tornar algo público, permitir acesso a esses dados ao resto do mundo – e, é claro, quando vemos adolescentes postando fotos de si mesmos bêbados ou algo assim, eles podem não ter a noção de que isso pode ser acessado pelo resto do mundo, potencialmente por muito, muito tempo. O Facebook ganha dinheiro reduzindo a distinção dessa linha entre privacidade, amigos e publicidade. E eles também armazenam os dados que você acredita serem restritivos aos seus amigos e às pessoas que você ama. Então, não importa o grau de publicidade que você gostaria de atribuir a seus dados, a cada vez que você clica no botão "publicar", dá esses dados primeiro ao Facebook, e em seguida permite o acesso a outros usuários. (ASSANGE et al. 2013, p. 59-60).

Este incentivo à publicidade individual contribui para a perda da privacidade e o controle do Estado. Por mais que a Internet sempre tenha sido considerada livre em sua cultura libertária[14], o ciberespaço foi colonizado pelos gigantes das telecomunicações (PÉREZ LUÑO, 2002, p. 108-110). Não cabe mais o ideal da Declaração de Independência do Ciberespaço[15]. Na Internet, como comenta Castells (2003, p. 149), uma multidão de agências de vigilância, e não um Big Brother registra o comportamento das pessoas, eis que para "[...] fazer valer seus interesses, o comércio e os governos ameaçam conjuntamente a liberdade ao violar a privacidade em nome da segurança.".

Ao lado deste grande desenvolvimento tecnológico alcançado por empresas da Internet, que implica na utilização massiva das tecnologias da informação e comunicação e, consequentemente, no tratamento de dados pessoais e o prevalecimento das questões de

[14] Segundo Manuel Castells, a cultura da Internet se estrutura em 04 (quatro) camadas: tecnomeritocrática, a cultura hacker, a cultura comunitária virtual e a cultura empresarial, e juntas "[...] elas contribuem para uma ideologia da liberdade que é amplamente disseminada no mundo da Internet.". (2003, p. 14). Em resumo, a cultura tecnomeritocrática se refere ao exercício de reputação da ciência acadêmica, de apresentação de seus resultados aos seus pares. A cultura hacker fomenta a inovação tecnológica mediante a cooperação livre entre os tecnomeritocráticos e os subprodutos empresariais que se difundem na Internet. As comunidades virtuais decorrem do envio de mensagens, salas de chats, jogos e conferências, enquanto seu uso comercial transforma a Internet, assim como esta transforma as empresas. (2003, p. 49).

[15] "Governos da Era Industrial, vocês gigantes aborrecidos de carne e aço, eu venho do ciberespaço, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nos reunimos.". (BARLOW, 1996, tradução nossa).

segurança, os Estados desenvolveram seus próprios programas de vigilância, como o *Echelon* e *Carnivore*. Nas palavras de Pérez Luño (2002, p. 107, tradução nossa.):

> *Echelon* é um sistema de interceptação das comunicações a nível mundial em que participam os Estados Unidos, o Reino Unido, Canadá, Austrália e Nova Zelândia. Uma das principais características, frente a outros sistemas de espionagem, são: sua capacidade para exercer um controle simultâneo de todas as comunicações. Todas mensagens enviadas por fax, telefone, Internet ou email, independentemente de seu remetente, pode ser captada mediante estações de interceptação de comunicações, o que permite conhecer seu conteúdo. Se trata de um sistema que funciona a escala mundial graças à colaboração e interação dos Estados supracitados, o qual possibilita uma vigilância a nível mundial das comunicações por satélite. Colocando em comum iniciativas, recursos técnicos e lógicos, custos e objetivos, representando uma implacável e completa rede de controle em escala planetária. *Carnivore* é um sistema de software e hardware com capacidade para localizar e perseguir as comunicações de um usuário de Internet. O sistema interfere a comunicação em um ponto estratégico, como é o ISP (Provedor de Serviço de Internet). Toda informação passa pelos ISP, servidores que todos os internautas utilizam para concertar-se a Internet. Cada palavra que escrevemos ou executamos sempre é reconhecida pelo ISP que nos dá acesso à Rede.

Além da expansão econômica e de vigilância da Internet nos anos 1990, juntamente com a expansão de programas de espionagem, o episódio de 11 de setembro de 2001, foi determinante para o desenvolvimento de tecnologias que passaram a acumular em muito maior proporção as informações (BAUMAN *et al,* 2015, p. 57). Estes programas de vigilância se utilizam do medo disseminado como tática de controle social pelos Estados para reduzirem a liberdade e aumentar o controle sobre as pessoas. Vale aqui o alerta de Pérez Luño (2002), por mais terríveis que tenham sido tais fatos, não podem servir para uma limitação injustificada dos direitos e liberdades civis, pois sem liberdade nunca se pode estar seguro.

Posteriormente, as revelações de Edward Snowden, em 2013, sobre a vigilância executada pela Agência de Segurança Nacional dos Estados Unidos confirmaram o que se suspeitava desde os anos 2001, que ela se estende através dos cabos de fibra ótica, que cobrem praticamente todos os meios de transmissão digital a longa distância hoje em uso, e também dos sistemas operacionais, como o Windows. Através desta espionagem, denunciou-se que eram manipulados mercados financeiros para manter irrigar campanhas militares americanas (POLITICS, 2013, p. 04).

Depois dos atentados terroristas, se intensificaram as práticas de espionagem e vigilância, sendo impulsionada pelas novas tecnologias. Mas como bem observa Dalla Favera (2018, p. 56), as pessoas que se encontram em observação constante são pessoas comuns e não terroristas, e os equipamentos informáticos por elas utilizados, como computadores, *notebooks*, *tablets,* celulares, são ferramentas e armas utilizadas pelos Estados para proceder a vigilância.

Ao permitir conhecer as práticas da agência de Segurança Nacional nos EUA (NSA) e seus programas de vigilância como o PRISM, e o Reino Unido e o Tempora, revelaram o descompromisso dos Estados com a democracia e o Estado de direito (BAUMAN *et al*, 2015). Nas palavras de Bauman *et al* (2015, p. 23) "Graças à documentação distribuída por Snowden e outros, sabemos agora mais do que sabíamos sobre o caráter e a extensão das práticas de coleta de informações de várias agências encarregadas de aumentar nossa segurança.". A segurança nacional, revela-se cada vez mais transnacional (BAUMAN *et al*, 2015, p. 20).

A despeito disto, recentemente, em 2019, a Anistia Internacional, movimento social global que realiza ações e campanhas de respeito e proteção aos direitos humanos, denunciou uma empresa israelense que vendia ferramentas para rastrear ativistas e críticos de vários países (ANISTIA INTERNACIONAL, 2019). A empresa alegou que comercializa softwares de espionagem com vários países do mundo com a finalidade de vigiar atitudes terroristas, e que se a utilização dos programas tem sido desviada para monitorar dissidentes políticos, isto decorre da má utilização pelos Estados.

Como ressalta Assange (ASSANGE, *et al*. 2013), sobre o lema da cultura "Cypherpunk"[16], "Privacidade para os fracos, transparência para os poderosos", diante da militarização do ciberespaço, o combate a vigilância em massa por parte dos Estados deve se dar através da construção de dispositivos que impeçam a interceptação, como a criptografia, e de leis que garantam os direitos das pessoas e forcem uma maior prestação de contas por parte do Estado e das empresas. (ASSANGE *et al*, 2013, p. 36).

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

[16] "Se voltarmos àquela época, no início dos anos 1990, quando tivemos a ascensão do movimento cypherpunk como uma reação às proibições da criptografia por parte do Estado, muitas pessoas acreditavam no poder da internet de proporcionar comunicações muito mais livres de censura se em comparação com a grande mídia. Mas o cypherpunks sempre souberam que, na verdade, com isso também vinha o poder de vigiar todas as comunicações. Temos agora uma maior comunicação *versus* uma maior vigilância. Uma maior comunicação significa que temos mais liberdade em relação às pessoas que estão tentando controlar as ideias e criar o consenso, e uma maior vigilância significa exatamente o contrário.". (ASSANGE *et al*, 2013, p. 36).

Se anteriormente, a vigilância era feita por alguns Estados, atualmente é feita por praticamente todos, em razão da comercialização da vigilância em massa. Evidenciado os riscos aos direitos fundamentais diante do fluxo informacional dos dados pessoais e a expansão da vigilância pelos Estados, necessária uma resposta jurídica no sentido de regular[17]. Mas há também de se ter uma mobilização social em torno destas violações aos direitos humanos, o que se revela no direito à proteção de dados pessoais e sua primeira geração de leis.

Antes de refletir sobre a regulação jurídica como indispensável para evitar os riscos da utilização das tecnologias da informação e comunicação e o direito à proteção de dados que dela decorre garantindo uma liberdade informática como um direito humano de terceira geração, aprofundar-se-á, no subcapítulo seguinte, os riscos da utilização dos dados pessoais pelo mercado.

2.2. O internauta nas tramas da rede: os dados pessoais em face do poder invisível do mercado

A utilização dos dados pessoais por parte do Estado no seu objetivo de controle social, muitas vezes obrigam as empresas a fornecer seus bancos de dados para fins de segurança interna e internacional. De outro lado, o simples fato de possuírem bancos de dados com grande capacidade de armazenamento, os coloca em uma situação privilegiada de informação e controle, com potencial para infringir a dignidade, a liberdade e a autonomia das pessoas por suas práticas agressivas de marketing e publicidade direcionada.

Como refere Lyon (2014), uma das tendências atuais do *Big Data*, que se verá mais adiante consiste em uma nova técnica de tratamento de dados, é a crescente integração de governos e vigilância comercial. Desse modo, o uso comercial e para fins de segurança estimulam a integração desta atividade, tendo neste contexto a utilização de dados para diferentes fins, e esta mudança pode alterar como os titulares dos dados podem interpretar sua privacidade ou o estabelecimento de limites legais para o uso secundário destes (LYON, 2014, p. 05-06).

[17] Em relação à respostas jurídicas, Castells (2003) ressalta que enquanto nos EUA, o congresso americano, sob fortes pressões de anunciantes e da indústria do comércio eletrônico rejeitou a obrigação das empresas excluir os dados obtidos dos usuários, cabendo a estes exercer o direito de exclusão, na União Europeia, uma ação governamental mais forte em favor da defesa do consumidor levou a uma lei de privacidade na qual as empresas não podem usar dados de seus consumidores sem o consentimento explícito deles. A regulação pela União Europeia dos usos dos dados das empresas que coletam de seus usuários protege numa medida muito maior que nos EUA, refletindo sobre o papel do Estado na tutela da privacidade e na regulação da utilização de dados pessoais (CASTELLS, 2003, p. 152).

O exercício da cidadania, diante da realidade do desenvolvimento tecnológico, se confunde com o conceito de privacidade. Neste sentido, afirma Doneda (2006, p. 142):

> Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais importância, passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade.

O conceito de privacidade não se encaixa em uma situação de direito subjetivo, mas sim, em uma situação subjetiva complexa, compondo interesses do titular e da coletividade, poderes e deveres, obrigações e ônus aos envolvidos. Esta situação subjetiva complexa passa, como lembra Fortes (2015, p. 154), da relação existente entre a proteção jurídica da privacidade e dos dados pessoais e a sociedade em rede, visto que "[...] a internet oferece ampla gama de oportunidades de coleta, análise, uso e armazenamento de dados pessoais, que são revertidos para múltiplas finalidades.".

A principal distinção das estruturas econômicas da primeira para a segunda metade do século XX é a presença das tecnologias da informação e sua difusão em todas as esferas sociais e econômicas, incluindo o fornecimento de uma infraestrutura global, permitindo que o conhecimento e a informação sejam as principais fontes de produtividade nas sociedades avançadas, caracterizando uma sociedade informacional (CASTELLS, 2000, p. 268). Estas transformações contextualizam a realidade, condicionada à tecnologia.

A "sociedade em rede" é um termo designado por Castells (2003) para explicar a época em que se vive, tendo como base a utilização da Internet e das tecnologias da informação e comunicação, e significando um novo paradigma de uma mudança radical da sociedade nos aspectos culturais, econômicos, políticos e sociais, assim como foi fundamental a eletricidade na Era Industrial (CASTELLS, 2003).[18] Trata-se de uma nova economia, com a Internet "[...] transformando a prática das empresas e sua relação com fornecedores e compradores, em sua administração, em seu processo de produção e em sua cooperação com outras firmas, em seu financiamento e na avaliação de ações em mercados financeiros." (CASTELLS, 2003, p. 56).

[18] "Assim, no modo agrário de desenvolvimento, a fonte do incremento de excedente resulta dos aumentos quantitativos da mão-de-obra e dos recursos naturais (em particular a terra) no processo produtivo, bem como da dotação natural desses recursos. No modo de desenvolvimento industrial, a principal fonte de produtividade reside na introdução de novas fontes de energia e na capacidade de descentralização do uso de energia ao longo dos processos produtivo e de circulação. No novo modo informacional de desenvolvimento, a fonte de produtividade acha-se na tecnologia de geração de conhecimentos, de processamento da informação e de comunicação de símbolos.". (CASTELLS, 2000, p. 53).

Há também outras interpretações sobre as sociedades atuais que se fazem necessárias descrever e guardam relação com a privacidade. Giddens (1991), por exemplo, vai trabalhar com a sociedade de risco, como já abordado no subcapítulo anterior. Doneda (2006, p. 38) lembra que este discurso é adequado às novas tecnologias, pois sua lógica "[...] não costuma ser a do indivíduo, visto que os custos e os meios de produção envolvidos requerem a quantidade que seja viável; e, portanto, podemos dizer que este sistema funciona tendo em vista basicamente os grandes números - dentro dos quais se diluem os indivíduos [...]". Importa dizer aqui, no que diz respeito aos riscos da utilização dos dados pessoais pelo mercado, que antes de qualquer coisa, estes decorrem do desenvolvimento do capitalismo, definido em um "[...] sistema de produção de mercadorias, centrado sobre a relação entre a propriedade privada do capital e o trabalho assalariado sem posse de propriedade, esta relação formando o eixo principal de um sistema de classes." (GIDDENS, 1991, p. 61), e do desenvolvimento do industrialismo, isto é, o "[...] o uso de fontes inanimadas de energia material na produção de bens, combinado ao papel central da maquinaria no processo de produção.". (GIDDENS, 1991, p. 61).

Esta concepção de sociedade de risco também é percebida através da análise do dinamismo da modernidade, advindo da transformação do tempo e do espaço. No mundo pré-moderno, em que pese a existência de calendários nos estados agrários, o tempo sempre era vinculado ao lugar ou identificado com ocorrências naturais regulares. Entretanto, com a invenção do relógio, no final do século XVIII, e o desenvolvimento da organização social do tempo, a mudança coincidiu com a expansão da modernidade (GIDDENS, 1991, p. 26). A aceleração do tempo seria uma das consequências da modernidade, com o predomínio do capitalismo como modo de produção nas sociedades, e a aceleração da produção industrial.

Deleuze (1992), ao comentar estas transformações, que ao invés de sociedades de risco as denomina como "sociedade de controle" [19], destaca como o marketing vira um instrumento de controle social promovendo uma mudança do capitalismo. Se nas sociedades disciplinares a vigilância na fábrica tinha como objetivo o menor salário e a maior produção, na atual sociedade de controle, as escalas de salário e a competição entre os empregados substituem a escola, e a forma anterior que se concentrava na produção e agora foca o produto (DELEUZE, 1992).

[19] "As antigas sociedades de soberania manejavam máquinas simples, alavancas, roldanas, relógios; mas as sociedades disciplinares recentes tinham por equipamento máquinas energéticas, com o perigo passivo da entropia e o perigo ativo da sabotagem; as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e o ativo a pirataria e a introdução de vírus. Não é uma evolução tecnológica sem ser, mais profundamente, uma mutação do capitalismo.". (DELEUZE, 1992, p. 223).

Bauman (2014), entendendo por esta linha, destaca a revolução gerencial, onde os gerentes se autodisciplinam, com a recompensa substituindo a punição e o policiamento através de tecnologias da informação e comunicação comercializadas, se constituindo em verdadeiros minipanópticos. Como lembra, "[...] em última instância, passar no teste de consumidor é condição inegociável para a admissão numa sociedade que foi remodelada à feição do mercado.". (BAUMAN, 2014, p. 27).

Diante deste cenário, a sociedade em rede comporta um risco com a vigilância exacerbada do mercado. A possibilidade de tratamento de dados pessoais pelas empresas decorre de uma estrutura social fomentada pela vigilância, concorrência e marketing no seio das sociedades industriais para as pós-industriais e também do desenvolvimento de novas tecnologias que proporcionam um controle social mais amplo.

Ao passo que nas sociedades disciplinares havia o risco de vigilância e controle exacerbado e limitação da liberdade, as novas tecnologias irão representar um risco muito maior diante da necessidade de controle social e vigilância, e a possibilidade de conversão de todas informações em dados pessoais. Estes, passam a ser um ativo diante das possibilidades de armazenamento, transferência, combinação e tratamento oferecidas pelas tecnologias da informação e comunicação, como o desenvolvimento do computador.

A despeito disto, Lash (2005) discorda deste entendimento de que a sociedade da informação seja caracterizada pela produção e uso intensivo do conhecimento e de uma série de bens e serviços pós-industrial, haja vista que suposta produção altamente racional pode gerar uma série de desinformações, descontrole e irracionalidade. No seu entender, a chave para a compreensão dos principais parâmetros da era da informação não é examinar a produção de bens e serviços com abundante conteúdo informacional, mas sim como *bytes* de informação, que implica na compressão da produção de informação e suas consequências como o descontrole (LASH, 2005, p. 22-23).

O pensamento de Lash sobre a centralidade da informação nas sociedades atuais vai ao encontro sobre as críticas de Lafontaine (2007) no que diz respeito à predominância do paradigma informacional após a segunda guerra mundial e do surgimento da cibernética. A definição de informação se estabeleceu com a cibernética como princípio básico e físico quantificável, formando os postulados básicos da informática. Esta possibilidade de armazenar a informação em *bytes* que revolucionou o tratamento de dados pessoais.

Além desse progresso quantitativo, conforme alerta Bioni (2016, p. 26), "[...] experimentou-se, também, uma mudança de ordem *qualitativa* no processamento de informações. Isto porque, a técnica binária permitiu que a informação fosse mais precisamente

organizada, facilitando, em última análise, o seu próprio acesso.". São a combinação destes dois fatores, progresso quantitativo e qualitativo, e, depois, com a criação da internet, que virtualizou a informação, que faz superar o modelo fordista de produção para instaurar uma novo "padrão sócio-técnico-econômico" (BIONI, 2016, p. 27).

Seja vista através da sociedade em rede, sociedade de risco, sociedade de vigilância ou de controle, há também de se considerar que o funcionamento da mídia desempenha papel fundamental na utilização de dados pessoais pelo mercado, tal qual necessita o Estado para o controle social. O desenvolvimento tecnológico e sua ligação com o mercado sinalizam a mesma dependência da ação da mídia e seu funcionamento e a necessidade de marketing e publicidade. O modelo pan-óptico de fazer sentir estar sendo espiado foi sendo substituído pela alegria de ser notado, através das mídias sociais cujo produto a ser exposto como marketing é a própria pessoa[20].

A Internet representa este modelo, de fonte de rendimentos das empresas de comércio eletrônico, sendo elas a publicidade e o marketing, mas também, os dados de seus usuários, demonstrando a presença dos modelos pan-ópticos reforçados por sua versão eletrônica, saindo das instituições totais da modernidade, como prisões, campos de concentração, para determinar categorizações de consumidores (BAUMAN, 2014). Como se pode observar, a vigilância no mercado objetiva a exclusão dos indesejáveis. Para Bauman (2014), o grande progresso da sociedade consumista foi a passagem da satisfação de necessidades para a criação de tentação, sedução e estímulo do desejo, possibilitando dirigir ofertas a pessoas ou categorias de pessoas.

Assim, aparecem atuando conjuntamente os modelos pan-ópticos, ban-ópticos e sin-ópticos de poder. O modelo pan-óptico de poder, identificado por Foucault como padrão ou estratégia de dominação no Estado moderno, em razão das tentações dos mercados de consumo, são substituídos pela autovigilância (BAUMAN, 2014, p. 44). Os modelos ban-ópticos, embora vistos como padrões nos postos de fronteira do Estado, também podem ser vistos nos padrões dos consumidores e indesejáveis, imprimindo sua lógica de preocupação com segurança e não do impulso disciplinador como no caso do pan-óptico (BAUMAN, 2014, p. 47).

---

[20] "Um bom exemplo, na verdade um exemplo arquetípico da interface entre esses dois tipos de técnica de vigilância institucionalizada é o software desenvolvido para uso em corporações que precisam processar as chamadas recebidas. Esse software permite que aqueles que fazem as chamadas sejam classificados e separados para tratamento diferenciado – de acordo com a promessa que representam (ou não) de aumentar os lucros da empresa. Os promissores não são obrigados a aguardar na linha, mas são imediatamente encaminhados a operadores seniores capacitados para tomar decisões na hora. Já os outros, os sem futuro, são submetidos a uma espera interminável, alimentados com mensagens tediosamente repetitivas, intercaladas por músicas reproduzidas *ad nauseam,* juntamente com a promessa gravada de serem encaminhados ao primeiro operador disponível, se o intruso sobreviver ao tratamento e ao escárnio nele implícito, por fim entrará em contato com um operador de nível mais baixo, sem poder para resolver o problema (normalmente uma queixa) que deu origem à chamada.". (BAUMAN, 2014, p. 54).

Já os modelos sinópticos substituem os pan-ópticos, predominando modelos de autovigilância (BAUMAN, 2014, p. 51). Um marketing eficaz "[...] exige o conhecimento das clientelas inadequadas para funcionar como alvo, da mesma forma que precisa identificar os 'alvos' mais promissores de seus esforços comerciais. Um marketing eficaz precisa *tanto* do sinóptico *quanto* do ban-óptico.". (BAUMAN, 2014, p. 54).

Como dito no primeiro subcapítulo, a produção cinematográfica sempre foi considerada uma arma para a propaganda pelo Estado, principalmente durante as duas guerras mundiais do século XX. Tendo os grandes templos do cinema desaparecido por volta de 1960, eles foram substituídos por grandes lojas de departamento de comércio (VIRILIO, 2005, p. 70). Mas, seus objetivos e seus efeitos se assemelham.

> Com a bomba de nêutrons, as populações urbanas perderam definitivamente o valor último de reféns nucleares. Abandonados pelos comandantes militares, os cidadãos não são mais os imortais da cidade, o cinema perdeu seu valor sintético e não é mais a massa negra da autoctonia guerreira propondo o Wallahla cinemático aos filhos da guerra, na comunhão dos vivos e dos mortos, simplesmente porque a dispersão comercial das imagens e dos sons destruiu essa extraordinária propriedade técnica do antigo cinema, essa formalização social obtida através da visão, que fazia com que houvesse apenas um único espectador em uma sala onde havia mil pessoas. (VIRILIO, 2005, p. 163).

Virílio (2005) observa que, sendo o indivíduo um alvo nervoso em potencial, a guerra faz com que se aprenda a controlar as emoções nervosas. Em síntese, esta ligação do cinema com a política e a guerra, dá início a era da "transpolítica", ou seja, "[...] o poder real passava agora a dividir-se entre a logística das armas e a logística das imagens e dos sons, entre os gabinetes de guerra e os escritórios de propaganda.". (VIRILIO, 2005, p. 136).

Como já dito, qualquer explicação da noção de privacidade deve estar fundada na percepção da relação do indivíduo com a sociedade. Com a ideia de privacidade passando a se desenvolver com a ideia de autonomia e uma forma de resistência do homem frente a tendência de massificação da sociedade industrial e a limitação do poder do Estado de intervir na vida das pessoas (DONEDA, 2006, p. 128), o controle da informação pelo mercado acaba por refletir sobre a cidadania, através da vigilância e controle social decorrente da utilização dos dados pessoais.

Fundamentalmente, a utilização das novas tecnologias irá forjar a cidadania e a vivência diária na sociedade em rede, devido ao intenso fluxo informacional e uma sociedade baseada no consumo e no marketing. A nova economia e as novas tecnologias acabam provocando novas assimetrias entre o Estado, o cidadão e o mercado. Nas palavras de Mendes (2008, p. 25), a "[...] ampliação da tecnologia reduziria inevitavelmente a privacidade pessoal, que, por sua

vez, somente poderia ser preservada com a contenção do desenvolvimento de tecnologias da informação.".

Castells (2003 p. 139) lembra que a Internet nasceu de um ideal libertário, prevalecendo o anonimato, mas que sua comercialização nos anos 1990 fez com que houvesse a necessidade de assegurar a identificação do usuário e proteger direitos de propriedade intelectual, permitindo o controle da comunicação por computadores através de softwares. Assim, uma variedade de tecnologias de controle emergiu dos interesses entrelaçados do comércio e dos governos, permitindo o desenvolvimento dos bancos de dados a partir dos resultados desta vigilância, que podem ser agregados, combinados e identificados, representando, o fim da privacidade, pois, "[...] a maior parte da atividade econômica, social e política, é de fato um híbrido de interação *on line* e física. [...] viver no pan-óptico eletrônico equivale a ter metade de nossas vidas permanentemente exposta a monitoramento.". (CASTELLS, 2003, p. 149). Neste sentido, descreve:

> Em síntese, os dispositivos tentam neutralizar o poder de criptografia. Proíbem softwares que são ferramentas pessoais de segurança [...]. Ampliam enormemente o poder do governo sobre interceptação de conversas telefônicas e de tráfego de dados. E obrigam os provedores de serviços da Internet a dispor de técnicas para o rastreamento de seus usuários por solicitação de agências governamentais, numa variedade muito ampla de situações e em circunstâncias vagamente definidas. Observe-se que, no conjunto, tudo corresponde a uma redução da privacidade da comunicação na Internet – a uma transformação da Internet de espaço da liberdade numa casa de vidro. (CASTELLS, 2003, p. 147).

Logo, se é verdadeiro que mais segurança significa menos liberdade, quanto mais se desenvolve a Internet, mais se fica sujeito à vigilância. Rodotà (2008, p. 113) observa que a contrapartida para obter serviços não se limita mais à soma de dinheiro solicitada, mas também há a necessidade se fazer uma cessão de informações. Assim, os riscos da sociedade de vigilância, geralmente ligados ao uso político das informações para controlar o cidadão, adquire agora novas formas de controle, tendo como objetivo não mais desencorajar determinados comportamentos, mas sim a classificação (RODOTÀ, 2008).

Os perfis são utilizados mais frequentemente para avaliar serviços que dizem respeito ao consumidor ou os usuários de serviços comerciais e bancários (RODOTÀ, 2008, p. 115). Tal medida constitui um novo desafio às minorias[21], tendo em vista esta classificação com

[21] "A plenitude da esfera pública depende diretamente da liberdade com a qual pode ser construída a esfera privada. Neste ponto, portanto, é necessário chegar a uma concepção de cidadania adequada à dimensão agora caracterizada pelo uso das tecnologias da informação e da comunicação. O primeiro problema volta a ser o da utilização das informações pessoais para a construção de perfis individuais ou de grupo.". (RODOTÀ, 2008, p. 115).

critérios de "normalidade" que tendem a controlar com a conveniência econômica[22] (RODOTÀ, 2008). Deste modo, o funcionamento do mercado na globalização exige para o exercício da cidadania e dos atos da vida civil o fornecimento constante de dados pessoais. O tratamento destes dados pessoais gera um risco ao cidadão, na medida em que pode implicar na restrição ou condicionamento de alguma atuação sua na vida em sociedade.

Por isso, há uma função sociopolítica da privacidade, que projeta, além da vida privada, um elemento de cidadania, evitando discriminação, por exemplo, na esfera pública por posições políticas (RODOTÀ, 2008). A privacidade não pode ser determinada pela referência a partir de critérios setoriais como o de consumo, devendo ser considerado um direito fundamental que não pode ser confiada à lógica da auto-regulamentação ou das relações econômicas (RODOTÀ, 2008).

Para Fortes (2016, p. 33), "[...] o direito à privacidade não é e não pode ser um estatuto imutável.". São justamente estas implicações do funcionamento da economia que irão modificando-o ao longo do tempo. O debate aqui sobre os riscos sócio-políticos da utilização dos dados pessoais não se refere ao desenvolvimento tecnológico como o cerne do problema. Mendes (2008, p. 26) assevera que "[...] não é a tecnologia em si a causa do problema da privacidade, mas as decisões que tomamos em relação à tecnologia.". É a regulação que irá definir as funções que a tecnologia deve assumir na sociedade.

Portanto, se faz preciso o uso das tecnologias da informação e comunicação para o exercício da cidadania. O mercado aproveita as informações fornecidas para aperfeiçoar seus produtos e sua publicidade. Diante deste aumento de poder das empresas em relação ao cidadão, é necessária uma proteção jurídica para que se possam exercer os direitos de um lado e não ser tolhido de outro. A privacidade adquire assim novos contornos, que não dizem mais somente respeito ao caráter individual. Doneda (2006, p. 15) observa que "Sem perder de vista que o controle a informação foi sempre um elemento essencial na definição de poderes dentro de uma sociedade, a tecnologia proporcionou a intensificação dos fluxos informacionais.".

Dentre as diferentes bases teóricas para o desenvolvimento do conceito de privacidade, como através da percepção de liberdade informática de Pérez Luño, ou ainda, através de matrizes teóricas que abordam o controle social pelo Estado e pelo mercado, é preciso reconhecer que as tecnologias da informação e comunicação (TIC) são ambivalentes. Ao mesmo tempo em que oferecem oportunidades, contemplam riscos na sua utilização.

[22] A revista *Science* publicou recente estudo sobre a utilização de um algoritmo que auxilia hospitais e seguradoras a administrar condições de saúde de seus pacientes, alertando que o sistema funcional com um viés racial, barrando pessoas negras de ter os cuidados de saúde necessários. (OLHAR DIGITAL, 2019).

Assim, uma das constatações sobre os novos riscos aos direitos humanos e fundamentais é que eles não são mensuráveis. Certamente uma regulação adequada deve levar em conta estas projeções. Em conta disto, resume bem Boaventura de Sousa Santos (2002, p. 80):

> Enquanto atitude epistemológica, a prudência é de difícil execução porque verdadeiramente só sabemos o que está em jogo quando já está, de fato, em jogo. Depois de dois séculos de utopismo automático da ciência e da tecnologia, esta dificuldade tem forçosamente de aumentar, mas, como já referi, a única alternativa é enfrenta-la. O princípio da prudência faz-nos uma dupla exigência. Por um lado, exige que, perante os limites da nossa capacidade de previsão, em comparação com o poder e a complexidade da *praxis* tecnológica, privilegiemos perscrutar as consequências negativas desta em detrimento das suas consequências positivas. Não deve ser-se nisto uma atitude pessimista e muito menos uma atitude reacionária. Umas das virtualidades do utopismo tecnológico é que hoje, sabemos melhor aquilo que não queremos do que aquilo que queremos. Se a nossa capacidade de previsão é menos limitada a respeito das consequências negativas do que a respeito das consequências positivas, é de bom senso concentrarmos o conhecimento emancipatório nas consequências negativas. Isto implica assumir perante ela – e esta é a segunda exigência – uma certa "hermenêutica de suspeição", como Ticouer lhe chamaria (1969: 67, 148-153): as consequências negativas duvidosas, mas possíveis, devem ser tidas como certas.

Esta atitude epistemológica de dar os riscos como certos amplia ainda mais a necessidade de proteção dos dados pessoais. Mas, além de os riscos não serem mensuráveis e a necessidade de tomada de precaução em relação a eles, a fim de investigá-los, é preciso antes de tudo reconhecer os limites do conhecimento, e estes "[...] obriga-nos a abordar a realidade partindo daquilo a que James chamou as 'últimas coisas', isto é, partindo das consequências, do impacto sobre o mundo da vida e sobre a nossa vida pessoal e coletiva.". (SANTOS, 2002, p. 109).

Observa-se, agora, a título de exemplificação, o caso Snowden e o surgimento do *Big data*, a possibilidade de publicidade direcionada por emoções e o escândalo Cambridge Analytica nas eleições americanas em 2016 (UNESCO, 2019, p. 18). Estes são os exemplos mais recentes de grandes riscos aos direitos fundamentais ocasionados pela utilização das tecnologias da informação e comunicação, especificamente do uso dos dados pessoais pelos Estados e pelo mercado na sociedade em rede.

Por volta do ano de 2011, quando o caso Snowden começou a ser revelado, apareceu o *Big Data,* que pode ser encarada como uma ferramenta poderosa para resolver diversos males sociais, mas por outro lado, constitui uma manifestação preocupante do Big Brother, permitindo invasões de privacidade e diminuindo as liberdades civis com um maior controle estatal e corporativo (BOYD, CROWFORD, 2012). O caso Snowden e suas revelações não fazem nada

mais que materializar uma prática que representa a síntese da ambivalência e dos riscos apontados pela literatura crítica das novas tecnologias.

Quanto mais informações e dadas pessoais disponíveis e tratadas nem sempre legalmente, mais expostos ficam os cidadãos ao controle social pelo mercado. Se os *bits* desmaterializam a informação e permitem assim sua introdução em computadores, implicando em uma virada exponencial na quantidade de informações processadas e de ordem qualitativa no processamento de informações (BIONI, 2019, p. 7-8), conforme já salientado, o *Big Data* seria o êxtase deste processo, associado ao volume, velocidade e variedade de dados, o que o diferencia de outras formas de tratamento (BIONI, 2019, p. 39-40). Boyd e Crawford (2012, p. 663, tradução nossa.), definem *Big Data* como:

> [...] um fenômeno cultural, tecnológico e acadêmico que se baseia na interação de: (1) *Tecnologia*: maximizando o poder computacional e a precisão algorítmica para reunir, analisar, vincular e comparar grandes conjuntos de dados. (2) *Análise*: baseando-se em grandes conjuntos de dados para identificar padrões e fazer reivindicações econômicas, sociais, técnicas e legais. (3) *Mitologia*: a crença generalizada de que grandes conjuntos de dados oferecem uma forma mais alta de inteligência e conhecimento que podem gerar insights anteriormente impossível, com a aura da verdade, objetividade e precisão.

O *Big Data* trata-se de uma realidade diante das novas possibilidade e técnicas de tratamento de dados. Sendo a vigilância impulsionada pelas tecnologias da informação e comunicação sob a crença de ordem e controle social, o *Big Data* também irá estimular a ampliação ainda maior destes mecanismos. Assim se pode observar a mitologia representada pelo *Big data* e sua suposta crença de sua eficiência. Observa-se que as práticas de *Big Data* não se reservam a coleta para fins limitados, específicos e transparentes, tal como objetiva os defensores da proteção de dados e da privacidade, e uma das tendências de vigilância ampliada pelas práticas do *Big Data* é a crescente integração de governos e vigilância comercial (LYON, 2014, p. 4-5).

Cabe aqui lembrar a velha lição de Ellul (1955, p. 285), ao anotar que o "[...] Estado tecnológico tem seus correspondentes diretos na própria sociedade uma vez que esta é construída sobre as técnicas, e no coração mesmo dos homens, adoradores da eficiência, da velocidade, da ordem ...". Virilio (1996a, p. 105) também irá dizer que o fundamentalismo não estará mais ligado à esperança no Deus, mas ao "tecno-culto", levando a realização de uma cibernética social fundada sobre o culto da informação, e ao assujeitamento discreto do ser pelas máquinas inteligentes.

Lyon (2014), em artigo refletindo sobre a relação entre as revelações de Snowden[23] e a vigilância e o *Big Data*, demonstra justamente esta a cumplicidade ambígua entre instituições de vigilância do Estado, como no caso a Agência Nacional de Segurança americana (NSA), e empresas da Internet. Snowden revelou que a NSA exigiu de empresas gigantes de telecomunicação a entregar "metadados" de milhões de clientes, proibindo que estes fossem comunicados disto (LYON, 2014, p. 02).

Lyon (2014) adverte que embora a definição de "metadados" ser imprecisa, refere-se a dados como endereços IP, identidade do contato, localização das chamadas ou mensagens e duração do contato, e que estas tendências de vigilância têm aumentado. No que diz respeito a algumas das divulgações:

> As práticas de vigilância reveladas por Snowden mostra claramente, se não completamente, que os governos - especialmente americano, britânico, canadense e possivelmente outras agências - participe de uma escala surpreendentemente grande monitoramento das populações e também como elas o fazem. Por um lado, a NSA envolve contratados para compartilham o ônus de seu trabalho e também reúne e extrai dados de usuários coletados por outras empresas, empresas de telefonia, internet e web. E em por outro, esse tipo de vigilância também significa que o a NSA e agências similares observam cookies e fazem login em formação. Assim, eles usam dados derivados do uso de dispositivos como telefones celulares ou mídias sociais e localização geográfica. O que os usuários inadvertidamente divulgam nessas plataformas - como Facebook ou Twitter - ou ao usar seus telefones, são dados utilizáveis para " segurança nacional " e fins de policiamento. Mas o mais importante de uma grande perspectiva de dados, metadados (veja a discussão abaixo) relacionados aos usuários que são recolhidos sem o conhecimento deles pelo simples uso dessas máquinas. Existem assim pelo menos três atores significativos nesse drama, agências de fomento, empresas privadas e, ainda que surpreendentemente, usuários comuns. (LYON, 2014, p. 02, tradução nossa.)

Da crítica literária à realidade das revelações de Snowden que, nas palavras de Menezes Neto (2016, 143), "[...] provaram a existência de uma estrutura mundial capaz de coletar e tratar informações em escala vista somente em filmes de ficção [...]", se descortinam os riscos aos direitos humanos e fundamentais. Segundo Lyon (2014), a tarefa atual não seria catalogar os aspectos benéficos do *Big Data*, mas advertir quais tipos de questões de vigilância tem de ser abordados.

---

[23] "No dia seguinte, artigos no Washington Post e The Guardian detalhou como o programa PRISM parecia dar à NSA acesso direto aos servidores de algumas das maiores empresas de tecnologia, incluindo Apple, Facebook, Google, Microsoft, Skype, Yahoo e YouTube. Os controles de criptografia e privacidade foram contornados com a ajuda das empresas (Gellman e Poitras, 2013). No Reino Unido, o programa Tempora parecia ser ainda mais como um arrastão, pois deu semelhante acesso para GCHQ (Sede Geral de comunicações; o parceiro britânico de a NSA nos " Cinco Olhos "). Juntos, seus cabos e as habilidades de escutas na rede são chamadas de " Upstream" e pode interceptar qualquer tráfego da Internet. O banco de dados permite que a informação seja extraída em tempo real e o tempo é chamado de " XKeyscore " (Lanchester, 2013). As revelações continuaram e o próprio Snowden afirmou (no início de 2014) que algumas das mais impressionantes divulgações ainda estão por vir.". (LYON, 2014, p. 02, tradução nossa.).

Os pesquisadores Boyd e Crawford (2012) publicaram artigo problematizando questões críticas acerca do *Big Data*, advertindo que assim como durante a revolução industrial o modo de produção Fordista limitava a capacidade dos trabalhadores pelas suas ferramentas, o *Big Data* também possui novas possibilidades e novas limitações. Embora, o *Big Data* "[...] ofereça às disciplinas humanísticas uma nova maneira de reivindicar o status de ciência quantitativa e método objetivo [...]" (BOYD, CRAWFORD, 2012, p. 08, tradução nossa.), ele ainda é subjetivo, pois sua quantidade de informação não significa necessariamente uma aproximação da verdade objetiva.

Ao passo que apesar de cientistas da computação reivindicar seu trabalho como negócios de fato e não de interpretação, ou, nas palavras dos autores, "[...] um modelo matematicamente sólido [...]" (BOYD, CRAWFORD, 2012, tradução nossa.), sabe-se que o *Big Data* não é autoexplicativo, eis ser preciso selecionar os dados, processo inteiramente subjetivo, e as metodologias específicas para interpretar os dados se sujeitam a todo tipo de debate filosófico. Por isso, Boyd e Crawford (2012) sustentam ser preciso reconhecer os limites da interpretação desses dados, pois existe possibilidade de erros, fontes não confiáveis da Internet propensas a perdas, alterações e interrupções, além do que a limitação também decorre de preconceito e má interpretação do pesquisador, devendo toda análise ter uma atenção a esta complexidade, independentemente do tamanho da base de dados, pois, "[...] só porque o *Big Data* nos apresenta grandes quantidades de dados não significa que questões metodológicas não são mais relevantes." (BOYD, CRAWFORD, 2012, p. 09).

Os autores (BOYD, CRAWFORD, 2012) utilizam como exemplo pesquisas no Twitter, em que se deve considerar que nem todos os usuários são ativos, pois se sabe, por revelação da própria plataforma, que cerca de 40 % dos usuários assinam o aplicativo somente para ouvir. Como descrevem, este aplicativo "[...] tornou uma fonte popular para minerar *Big Data*, mas trabalhar com dados do Twitter apresentam sérios desafios metodológicos que raramente são abordados por aqueles que o abraçam.". (BOYD, CRAWFORD, 2012, p. 10, tradução nossa.).

Entretanto, isto não significa que combinações de dados não ofereça informações valiosas, como as de bancos públicos que podem gerar graves violações de privacidade, e que, por outro lado, pequenos dados também não podem revelar informações relevantes (BOYD, CRAWFORD, 2012). Como advertem, existe uma dificuldade em apontar os danos que a violação da privacidade pode causar, e os riscos reais dos abusos de tais dados são difíceis quantificar, tendo surgido iniciativas como comitês éticos de pesquisa, o consentimento, de sorte que a "[...] Era do *Big Data* está apenas começando, mas já é importante começarmos a

questionar as suposições, valores e preconceitos dessa nova onda de pesquisa.". (BOYD, CRAWFORD, 2012, p. 10, tradução nossa.).

Se o *Big Data* se torna uma realidade diante das revelações de Snowden e passa a ser uma tendência em uma forma inovadora de tratamento de dados pessoais, mais razão se deve procurar a melhor regulação jurídica sobre o tema. Caso contrário, mais expostos estarão os direitos humanos e fundamentais do cidadão. Os modelos de negócio baseados no *Big data* possibilitam um controle "[...] permanente sobre os consumidores, com dados obtidos e tratados em tempo real, conservados por tempo indeterminado, com vista a obter informações ainda não evidentes, muitas delas nem sequer previstas no momento de recolha e tratamento inicial dos dados.". (MASSENO, 2019, p. 8). Umas das consequências, por exemplo, é analisada por Masseno (2019, p. 6):

> [...] com programas informáticos dotados de Inteligência Artificial capazes de manter um diálogo com um interlocutor humano, os custos de transação reduziram-se até ao ponto em que se tornou viável negociar individualmente cada uma das cláusulas contratuais. Mais ainda, o consumidor passou a ter perante si um interlocutor com um conhecimento muito aprofundado das necessidades e aspirações, porventura maior que o próprio tem de si, pelo menos conscientemente. O que vem desiquilibrar, de um modo ainda mais acentuado, as posições das partes nas relações de consumo.".

Não bastando a repetição de ampliação da vigilância das novas tecnologias reveladas pelo caso Snowden, e o *Big Data* e a ligação entre os Estados e o mercado, tem-se desenvolvido novas formas de controle da informação e utilização dos dados pessoais de uma forma que ainda não havia sido descrita por estas revelações. Ocorre que o marketing e a publicidade como instrumentos de controle social, amplificam suas tendências com a possibilidade de armazenamento e tratamento de estímulos neurológicos e sensoriais que tem se desenvolvido com as novas tecnologias, demonstrando um risco de uma publicidade agressiva e individualizada baseada em emoções.

Em artigo publicado no jornal Folha de São Paulo, Morozov (2013) problematiza o perigo da publicidade baseada em emoções em um contexto onde, até pouco tempo atrás, os sensores eram capazes de registrar o que se tecla, como se movem os mouses, mas não eram capazes de registrar as sensações das pessoas. Este histórico de navegação é usado para prever o que se deseja fazer e priorizando determinados resultados de busca no futuro. No entanto, hoje em dia os sensores podem captar muitas outras dimensões das atividades das pessoas, como indicadores neurofisiológicos que podem informar a quantidade de calorias queimadas, indicadores emocionais que podem informar se a pessoa está ansiosa ou excitada.

Atualmente, a publicidade baseada em emoções é uma realidade, diante da vigilância imperativa das pessoas, agora às suas próprias emoções (BIONI, 2019, p. 24). Este ajuste dos aparelhos com base nas sensações das pessoas faz-se perguntar o que dizer sobre os anúncios exibidos às pessoas, diante da proliferação da "Internet das Coisas" (IoT), conceito este relacionado a uma nova era da internet chamada web 3.0 (MAGRANI, 2018, p. 61). Estas tecnologias são capazes de, conforme alerta Magrani (2018, p. 73) "[...] integrar gradativamente as tecnologias ao ser humano, podendo envolver até sentimentos e emoções.". Nas palavras de Morozov (2013, p. 01):

> Considere apenas dois produtos que recentemente ganharam destaque na mídia de tecnologia: um carro que desacelera quanto sente que você está dirigindo sem prestar atenção, e uma mesa que registra quantas calorias você queima e ajusta sua altura com base nisso. É verdade que o carro com sensor de atenção é apenas um modelo de teste que requer que o motorista use um capacete especial, mas é possível imaginar o número de sensores incorporados à coluna do volante que tornaria menos visível o processo de detecção de atenção. (A Toyota já testou sensores como esses em 2011, enquanto a Ford vem testando monitores de batimento cardíaco incorporados ao assento do motorista.). Já a mesa é um produto real (ainda que caro e exclusivo). Ao contrário das mesas convencionais, ela busca criar interação com o usuário ao "mudar as coisas durante o dia, subindo um ou dois centímetros, bem gentilmente". Se combinada a fluxos de dados dos demais sensores de nossas vidas, a mesa pode ser transformada de um tedioso lugar de trabalho em uma máquina de exercícios.

Para esta problemática de coleta e armazenamento de base emocional não estão preparadas as autoridades regulatórias, hoje ocupadas com os problemas de privacidade criados pelas informações textuais, mas, deve-se estar atento, pois, a forma de publicidade "[...] altamente personalizada e de base emocional que se torna possível em um mundo que qualquer superfície de toque possa adivinhar como nos sentimos, e nos exibir um anúncio relacionado a esses sentimentos, deveria nos levar a reconsiderar." (MOROZOV, 2013, p. 03). Por outro lado, Magrani (2018, p. 104) adverte que "As empresas desenvolvedoras de dispositivos de IoT devem ter como princípio norteador o aprimoramento de sua capacidade de assegurar a segurança e a privacidade dos usuários nas fases de coleta, tratamento e compartilhamento de dados.".

Assim, o *Big Data* e a publicidade direcionada baseada em emoções são exemplos da expansão da vigilância na atualidade, em que os dados acabam sendo utilizados para diversas finalidades. Esta vigilância acaba por limitar a liberdade e a autonomia das pessoas, acabando por fazer prevalecer uma comunicação simbólica na sociedade que em nada contribui para a democracia. Não é difícil perceber os riscos aos direitos humanos e direitos fundamentais decorrentes destes casos concretos.

Por fim, o escândalo Cambridge Analytica, na eleição estadunidense de 2016, é paradigmático no que diz respeito aos riscos associados à segurança dos dados pessoais e à privacidade do cidadão. Conforme divulgado pela *Federal Trade Commission* (FTC - Comissão Federal de proteção ao consumidor e concorrência dos Estados Unidos), esta empresa teria traçado perfis e direcionado eleitores americanos, e atualmente está sendo processada por alegações enganosas sobre as informações pessoais dos consumidores.

Isto foi possível com o uso dos dados dos usuários do Facebook. Em 2012, a rede social já havia firmado um acordo com a FTC, após ser acusada de várias violações relacionadas à privacidade, como deturpações sobre a segurança das informações dos consumidores e a extensão do compartilhamento de seus dados pessoais. Umas das formas de deturpação eram suas políticas de privacidade e as escolhas dos usuários, eis que se constatou que ainda que os consumidores restringissem o acesso às informações apenas a "amigos", era possível aos aplicativos utilizados por estes "amigos" acessar as informações daquele sem a divulgação adequada que outras configurações permitiam este acesso.

> Em outras palavras, suponha que o Consumidor A restrinja o acesso a amigos e designe o Consumidor B como amigo. Se o Consumidor B usou um aplicativo específico no Facebook - digamos, um jogo - o desenvolvedor do jogo pode acessar informações sobre o Consumidor A, incluindo dados designados como particulares. (FEDERAL TRADE COMMISSION, 2019a, p. 02).

Como as práticas teriam continuado em que pese o acordo de 2012, no ano de 2019 foi-lhe aplicada uma penalidade civil de U$ 5 bilhões, sendo a maior multa a uma empresa em qualquer lugar por violar a privacidade dos consumidores. O julgamento foi disponibilizado pela FTC, em 24 de julho de 2019, tendo a empresa reconhecido as violações apontadas ocorridas anteriores ao acordo (FEDERAL TRADE COMMISSION, 2019c).

Há várias obrigações ao Facebook, no presente acordo firmado, sobre a proteção da privacidade. Dentre elas, que a empresa não deturpe até que ponto mantém a privacidade nas configurações do usuário e a segurança dos seus dados, que realize relatórios de riscos da atividade e do compartilhamento de suas informações com terceiros e que faça avaliações independentes do programa de privacidade (FEDERAL TRADE COMMISSION, 2019c).

A empresa Cambridge Analytica, desenvolvida por pesquisadores que sugeriam que as curtidas de uma pessoa em páginas publicadas no Facebook poderiam ser usadas para prever uma série de traços de personalidade, surge para oferecer perfil de eleitor e serviços de publicidade direcionada e outros para campanhas e clientes dos EUA. De acordo com o que foi informado sobre a denúncia da FTC, ela teria utilizado um aplicativo para coletar dados do

Facebook, atingindo entre 250.000 (duzentos e cinquenta mil) e 270.000 (duzentos e setenta mil) usuários nos EUA, e que incluindo os dados obtidos dos amigos destes na rede social, atingiria cerca de 30 milhões de consumidores norte-americanos identificáveis (FEDERAL TRADE COMMISSION, 2019b).

Este caso demonstra as sérias consequências de quando as empresas enganam os consumidores sobre o uso de suas informações pessoais. Através dos dados obtidos de maneira ilegal, as empresas aprimoram a formação de perfis para utilização de publicidade dirigida em eleições. A publicidade dirigida através da formação de perfis com informações agregadas de bancos de dados também é referida no Relatório Mueller, do Senado Federal Americano, que descreveu a campanha abrangente e sistemática da Rússia por Donald Trump nas eleições americanas de 2016 (U.S. DEPARTMENT OF JUSTICE, 2019).

A interferência teria ocorrido através de uma empesa chamada Agência de Pesquisa da Internet (IRA), baseada em São Petersburgo, na Rússia, e financiada por oligarcas deste país. Segundo o relatório do Senado americano, utilizando-se de contas de mídia social e grupos de interesse para semear a discórdia no sistema político dos EUA, fez-se compras de anúncios políticos em mídias sociais, e realizou-se comícios políticos dentro do país em nome de pessoas e entidades deste. O relatório descreve que se estimula que a agência IRA possa ter alcançado até 126 milhões de pessoas através de suas contas no Facebook.

Timothy Snyder (2019), professor de história da Universidade de Yale, em artigo recente publicado na revista The New York Review of Books, reflete sobre a ascensão do poder dos dados e sua capacidade de influenciar uma eleição. Conforme descreve o artigo, através de perfis e publicidade dirigida, é possível perceber como os algoritmos entram nas mentes e coordenam as ações das pessoas com as preferências de vários anunciantes (SNYDER, 2019, p. 21, tradução nossa).

> Na década de 2010, a Internet trouxe ficção gratuita, misturada com histórias ocasionais de jornais famintos por conteúdo, classificadas por plataformas de acordo com as preferências psicológicas e vulnerabilidades do indivíduo, nunca vistas da mesma maneira por ninguém e nunca mais acessíveis na mesma combinação. Nos Estados Unidos, em 2016, a principal fonte de notícias foi o Facebook, o veículo de entrega preferido da Rússia. Havia cerca de cinco vezes mais contas falsas no Facebook do que os eleitores americanos, que não sabiam disso. Nem foram informados de que os estrangeiros estavam manipulando seus feeds de notícias. Os americanos que perderam o jornalismo local leram e confiaram no Facebook como se fosse um jornal. [...] Graças apenas ao Facebook, a Rússia alcançou cerca de 126 milhões de cidadãos americanos naquele ano, quase tantos quantos votaram (137 milhões). A Rússia (e outros atores) expuseram os americanos à propaganda na Internet de acordo com as próprias suscetibilidades desses cidadãos, que inadvertidamente revelaram por suas práticas na Internet.

Este episódio das eleições americanas de 2016 demonstram os riscos advindos das grandes bases de dados e seu poder. Através de mecanismos que distorcem as opções de privacidade do usuário, os perfis de comportamento são utilizados tanto no setor comercial, como no político, com seu modo de revelar suas práticas. Com a propaganda e o seu controle emocional, o direcionamento de cidadãos americanos fragiliza o processo democrático, eis que não se pode dizer que elas foram livres, limitando assim os direitos civis e políticos das pessoas, além de sua autonomia e livre desenvolvimento de suas personalidades.

Esta mesma estratégia de formação e utilização de perfis através de imensa base de dados obtidos no Facebook pode ter sido utilizada nas eleições britânicas sobre o referendo de permanência na União Europeia. Em investigação realizada pelo parlamento britânico[24], publicada em 18 de fevereiro de 2019, intitulada como "Desinformação e Fake News", tratou-se da relação dos poderes dos indivíduos sobre sua privacidade, demonstrando como as escolhas políticas podem ter sido afetadas e influenciadas por informações na Internet no país e em diversos outros, como o Brasil.

Conforme seu relatório de investigação (HOUSE OF COMMONS, 2019, p. 06 e 96, tradução nossa.), a forma como a empresa Facebook coletava dados dos usuários violando suas privacidades através de distorções das informações ao consumidor corroborou para a utilização de publicidade direcionada no referendo de permanência na União Europeia. Dentre as principais conclusões, destaca-se a avaliação de necessidade de maior transparência das empresas de mídia social sobre seus próprios sites e como eles funcionam.

Do mesmo modo, no Brasil, a *Coding Rights* (2018), organização não governamental, realizou uma pesquisa para o projeto internacional "Dados Pessoais e influência política", entrevistando empresas de publicidade que atuavam na prestação de serviços eleitorais no país. A maioria destas empresas destaca que as diversidades de informações geradas na Internet representam um excelente ponto de partida para seus negócios, considerando o cruzamento de banco de dados contendo informações públicas, como aquelas utilizadas para políticas públicas, dentre elas as informações do censo pelo Instituto Brasileiro de Geografia e Estatística (IBGE),

[24] Como referido no relatório, "Em uma democracia, precisamos experimentar uma pluralidade de vozes e, criticamente, ter as habilidades, a experiência e o conhecimento para avaliar a veracidade dessas vozes. Embora a Internet tenha trazido muitas liberdades por todo o mundo e uma capacidade sem precedentes de comunicação, ela também carrega a capacidade insidiosa de distorcer, enganar e produzir ódio e instabilidade. Ele funciona em uma escala e a uma velocidade sem precedentes na história humana. Uma das testemunhas em nossa investigação, Tristan Harris, do Center for Humane Technology, com sede nos EUA, descreve o uso atual da tecnologia como "seqüestrar nossas mentes e a sociedade". Em vez disso, devemos usar a tecnologia para libertar nossa mente e usar a regulamentação para restaurar a responsabilidade democrática. Devemos garantir que as pessoas fiquem no comando das máquinas..". (HOUSE OF COMMONS, 2019, p. 06 e 96, tradução nossa.)

da Serasa Experian e do Facebook. Dentre as empresas entrevistadas pela pesquisa, estava a Cambridge Analytica, porém, antes do escândalo tornar-se público.

Devido ao aperfeiçoamento da coleta, tratamento, armazenamento e transferência dos dados pessoais, a privacidade e a proteção de dados passa a ser um grande desafio para os Estados e para os direitos humanos. Como se percebe, o uso de análise de dados em campanhas políticas revela que as empresas desconsideram a privacidade dos eleitores. Deste modo, é possível perceber a pluralidade de situações de direitos violados conforme aponta um conceito plural de privacidade, envolvendo intimidade, liberdade, autonomia, ausência de controle sobre as informações, utilização dos dados pessoais em finalidades obscuras e enfraquecimento da democracia.

É neste sentido que Lyon (2014) também comenta ser difícil dizer com exatidão as consequências para a vigilância da ampla adoção do *Big Data* devido à combinação de softwares de baixo custo e algoritmos, sendo uma possibilidade crescente a vigilância automatizada, sendo que a utilização do aumento dessas bases de dados ainda é desconhecida. O que se sabe é que "[...] uma lógica neoliberal de controle se encaixa perfeitamente com a maneira como os indivíduos são 'inventados' por dados.". (LYON, 2014, p. 06, tradução nossa.). O autor (LYON, 2014) também aponta que a vigilância do *Big Data* não possui foco apenas no corpo ou na população, mas para definir iniciações em nossas atividades diárias, e contribui para o controle de tipo cibernético, que é assumido como comportamento normal e correto e incorporado em circuitos de consumidor. Desde os anos 1990, vem se desenvolvendo técnicas de gerenciamento de riscos e práticas voltadas à antecipação de eventos futuros, e o episódio 11 de setembro de 2001 marcou uma vigilância muito maior, eis que "[...] o *Big Data* se baseia nesses modos já existentes de vigilância antecipada na tentativa de criar novos conhecimentos usando o poder estatístico de grandes números para ajudar a entender os detalhes fragmentados das vidas individuais.". (LYON, 2014, p. 07, tradução nossa.).

Por estes motivos, a observação aos riscos sócio-políticos diante da utilização dos dados pessoais pelo mercado é reveladora da capacidade de violação de direitos humanos e fundamentais do cidadão, e se justifica o "[...] receio de que as novas tecnologias promovam uma estrutura vertical das reações sócio-políticas, levando à despersonalização do cidadão e à alienação política.". (NASCIMENTO, 2012, p. 102). Em suma,

> [...] os algoritmos aderem assim como nos seguem, produzindo cada vez mais informações para fazer tornar os dados do usuário mais eficazes. Os usuários descobrem pode-se dizer, que o preço de nossa liberdade em contexto político e de consumo é nossa modelagem ou condicionamento por algoritmos. (LYON, 2014, p. 07, tradução nossa.).

Neste aspecto, acabam prevalecendo preconceitos neoliberais como de “pobres merecedores”, perfis de bandidos e terroristas, que persistem como categorias desagradáveis e ampliando-as com a confiança cega depositada em sistemas automatizados e atuarial[25] (LYON, 2014). Os riscos cada vez mais se assemelham as distopias das obras literárias de “1984” de Orwell (1949), onde o Estado controlava toda a informação, e “Admirável Mundo Novo” de Huxley (1932), onde se vive em uma sociedade assustadoramente em ordem conforme suas classificações de perfis genéticos.

Há de ter em conta que se prevalecer o lado perverso da Internet, nas palavras de Rodotà (2008, p. 194),

> [...] corre-se o risco de que a promessa tecnológica se transforme na mais pesada das limitações, dando relevância social à tese que pretende a técnica como portadora de uma potência irresistível, destinada a impor sua própria lógica onde quer que seja. A tecnologia é sedutora, já que a sua incessante produção de novidades se apresenta precisamente como “a” solução de qualquer problema pessoal, social, econômico, político, cultural: e não há dúvidas que as propostas tecnológicas sejam fruto de uma análise de necessidades e de interesses reais. Mas é necessário justamente questionar se a realidade deva ser abordada somente através das lentes da técnica, tornando *substancialmente vinculantes* as soluções que esta propõe, ou se a política deva ter o seu filtro. Porém, uma política seduzida pela tecnologia torna-se sua refém, renuncia às suas próprias capacidades.

Os riscos são incertos, mas exemplos concretos destas ameaças já existem. A impossibilidade de solução do problema não impede a adoção de medidas para mitigar os riscos do progresso tecnológico e o tratamento de dados, “Do mesmo modo, o direito penal não impede o crime nem o crime organizado.”. (FRYDMAN, 2014, p. 93, tradução nossa.). Como afirma Doneda (2006, p. 39), a primeira constatação a ser explicitada é que o desenvolvimento tecnológico cria novas relações a serem reguladas pelo direito. Sendo assim, é preciso ser pragmático e consciente das limitações e diversas possibilidades de o ordenamento jurídico tratar a matéria (DONEDA, 2006, p. 23). Em segundo, “As características da sociedade informatizada se juntam em um ponto de profunda interconexão entre os processos tecnológicos, políticos, jurídicos, econômicos e sociais [...]” (PÉREZ LUÑO, 2003, p. 99). Os riscos aos direitos fundamentais e as repercussões sócio-políticas das novas tecnologias revelam ser necessário um debate interdisciplinar (PÉREZ LUÑO, 2003, p. 99).

---

[25] “[...] o *calcanhar de Aquiles* da *Política Criminal Atuarial* resume-se à inevitável *margem de erro dos prognósticos de risco*, encarnada em dois inconvenientes personagens: de um lado, *os falsos-positivos*, isto é, as pessoas que são equivocadamente rotuladas como de *alto risco* ou *perigosas*, embora não representem nenhuma ameaça real à sociedade; de outro, os *falsos-negativos*, como são chamadas os *reincidentes crônicos* e *violentos* erroneamente *perfilados* por *instrumentos atuariais* como de *baixo risco.”* Sobre a política criminal atuarial, ver mais em: “Política Criminal Atuarial: A Criminologia do fim da história”, tese de Maurício Stegemannn Dieter (2012).

O tratamento de dados pessoais tem implicações que vão além da possibilidade de um estrito controle individual. Uma das consequências sócio-políticas do desenvolvimento tecnológico é o reconhecimento da necessidade de uma liberdade informática, o que na visão de Pérez Luño (2000, p. 64), originam as primeiras leis de proteção de dados, e posteriormente, como se observará no capítulo seguinte, evoluíram em gerações, tais quais as gerações de direitos humanos. Segundo o autor, estas seriam estratégias reivindicativas dos direitos humanos de terceira geração, devido à contaminação das liberdades diante do uso das novas tecnologias.

Em comum com o conceito plural de privacidade e perspectivas teóricas sobre o controle social, as novas condições de exercício dos direitos humanos determinam uma nova forma de cidadania no Estado de direito e as sociedades tecnológicas. Além desta mudança de dimensão, Pérez Luño (2000, p. 65) observa a mudança e surgimento de instrumentos jurídicos e procedimentos dirigidos a positivação e proteção dos problemas relacionados ao direito e as novas tecnologias.

Se anteriormente os direitos individuais estavam fundamentados na liberdade, e os direitos sociais, econômicos e culturais na igualdade, a terceira geração de direitos humanos é pautada pela solidariedade e necessitam de esforços em escala planetária. Por isso, a convergência internacional sobre as leis de proteção de dados se destaca, mas também, a criação de Autoridades Nacionais de Proteção de Dados tem sido um procedimento protagonista na defesa dos direitos e liberdades de terceira geração (PÉREZ LUÑO, 2013, p. 179-180).

Como enfatiza Pérez Luño (2013), seu sistema oferece a vantagem de proteção efetiva dos direitos humanos, sendo difundida em vários países. Suas principais funções, além das típicas de Estado, são de informar o parlamento das dinâmicas e adaptações do desenvolvimento tecnológico, orientar os cidadãos sobre os procedimentos de tutela das liberdade e proteção de dados pessoais e prevenir ameaças aos direitos humanos evitando danos e agressões de difícil reparação.

Posto que o tratamento de dados tem sido cada vez mais sofisticado diante surgimento de novas técnicas e os consequentes riscos aos direitos humanos e direitos fundamentais e a privacidade, se revelam ainda mais importantes as leis de proteção de dados que no contexto em que surgiram. Assim como, ainda mais necessárias a criação de autoridades de proteção de dados como estratégia inovadora de efetiva proteção e organização dos mecanismos de tutela, o que serão aprofundados no segundo capítulo, em perspectiva comparada entre a União Europeia e o Brasil.

3. O TRATAMENTO JURÍDICO DOS DADOS PESSOAIS: a atuação da Autoridade Nacional de Proteção de Dados em perspectiva comparada

O segundo capítulo desta dissertação visará investigar o tratamento jurídico da proteção de dados pessoais existentes na União Europeia e no Brasil, em perspectiva comparada, verificando como são tratados elementos como a autodeterminação informativa e a gestão do risco, com ênfase para a atuação da Autoridade Nacional de Proteção de Dados. Conforme conceito legal, o tratamento de dados pessoais é:

> Artigo 4.º. **Definições. [**...] uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjunto de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição [...]. (UNIÃO EUROPEIA, 2016).

Situada a questão de como o tratamento de dados pessoais podem violar direitos humanos e direitos fundamentais em uma economia e uma sociedade cada vez mais dependente do fluxo informacional, a principal característica da autodeterminação informativa é assegurar o seu controle ao cidadão de forma que ele autorize seu uso em um fluxo informacional que não agrida o livre desenvolvimento da personalidade (BIONI, 2019, p. 110). O reconhecimento do direito fundamental à autodeterminação informativa sobre os dados pessoais estabelece "[...] um corolário do direito geral de personalidade e dignidade humana [...]" (FORTES, 2016, p. 154), e equivale, nos termos de que trata Pérez Luño, e visto no primeiro capítulo, à uma liberdade informática, tendo "[...] uma importância indiscutível para a sociedade contemporânea.". (LIMBERGER, 2007, p. 103).

De outro lado, a gestão do risco representa uma nova abordagem da proteção de dados pessoais centrada na regulação do risco, envolvendo estratégias regulatórias de mitigação a riscos a direitos e liberdades em uma perspectiva coletiva (ZANATTA, 2017, p. 181). Com a aprovação, em 2019, da Autoridade Nacional de Proteção de Dados e do Conselho Nacional de Proteção de dados Pessoais e da Privacidade brasileiros, pretende-se discutir o modelo de regulação delineado, suas potencialidades e limites para que o Brasil alcance um nível de tratamento jurídico compatível com o existente na União Europeia e adequado do tema. Assim, em sua primeira parte, será descrito o marco regulatório dos dados pessoais na União Europeia. Na segunda parte, investigar-se-á a trajetória brasileira na proteção de dados pessoais em perspectiva comparada e as promessas normativas para a atuação da autoridade nacional.

3.1. O marco regulatório dos dados pessoais na União Europeia: o papel da Autoridade Nacional de Proteção de Dados

Antes de analisar-se o tratamento jurídico decorrente da proteção de dados pessoais na União Europeia (UE), deve-se dizer que o bloco europeu se trata de um novo modo de organizar as relações entre os Estados, tendo profunda conexão com o seu passado histórico[26]. Suas fases, em um breve resumo, passam pela criação de um mercado interno no campo econômico, logo após a segunda guerra mundial, como visto no primeiro capítulo, e pela eleição do parlamento europeu e pela adoção e aprovação, no ano de 2009, do Tratado de Lisboa no campo político.

Em que pese suas peculiaridades que não serão aqui exploradas, por não ser o objetivo da presente dissertação, há de se ressaltar que o marco regulatório da proteção de dados pessoais na União Europeia é um fator importante para a consolidação do mercado comum europeu. O direito à proteção de dados é previsto no Tratado de Lisboa[27], Tratado sobre o Funcionamento da União Europeia[28], Tratado que estabelece uma Constituição para a Europa[29] e Carta dos Direitos Fundamentais da União Europeia (analisado posteriormente, devido à sua importância). Conforme se observará a seguir, os países da União Europeia foram os pioneiros em considerar a proteção de dados com um direito fundamental, impulsionando sistemas de proteção de dados em outros países (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010).

---

[26] "Trata-se, realmente, de um processo que permitiu superar os mais graves aspectos degenerativos da vida política, econômica e social, que caracterizam a crise do Estado nacional no período entre as duas guerras: a colaboração entre os Estados, em vez do nacionalismo e do imperialismo, a expansão das forças produtivas no mercado comum, em vez da estagnação econômica, do protecionismo e da autarquia, e a democracia, em vez do fascismo.". (BOBBIO *et al*, 1998, p. 1271). Note-se que a partir da necessidade de governamentalidade pelos Estados e elaboração de políticas públicas, também se desenvolve como fator econômico a união dos países europeus em um bloco. Desde, já se observa e ressalta-se a importância do fator econômico em toda a complexidade envolvida no tema da proteção de dados.

[27] "Artigo 39. º. Em conformidade com o artigo 16º do Tratado sobre o Funcionamento da União Europeia e em derrogação do n.º 2 do mesmo artigo, o Conselho adota uma decisão que estabeleça as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação do presente capítulo, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controle de autoridades independentes.". (UNIÃO EUROPEIA, 2007).

[28] "Artigo 16º. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controle de autoridades independentes. As normas adotadas com base no presente artigo não prejudicam as normas específicas previstas no artigo 39. º do Tratado da União Europeia.". (UNIÃO EUROPEIA, 2009).

[29] "Artigo I-51º. **Proteção de dados pessoais.** 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. A lei ou lei-quadro europeia estabelece as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados. A observância dessas normas fica sujeita ao controle de autoridades independentes.". (UNIÃO EUROPEIA, 2004)

Existem dois modelos predominantes e distintos de proteção de dados (DONEDA, 2006). O modelo europeu de proteção de dados pessoais, baseado, até então, na Diretiva 95/46/CE, e agora no Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) [30], e, o modelo norte-americano, fracionado, devido à sua complexa estrutura federativa[31]. A atual legislação europeia se destaca, e de acordo com Mendes (2018, p. 2), "[...] passam a prever novos mecanismos como relatórios de impacto, códigos de boas condutas, certificações e programas de governança, [...] normas que incentivam a implementação do conceito de *Privacy by Design* [...].".

Como explica Doneda (2006, p. 227), o modelo europeu "[...] representa um padrão mínimo de proteção em toda a área da União Europeia, desenvolvido tendo como base a experiência de alguns países europeus que já haviam legislado sobre a matéria.". As gerações de leis nacionais, o que se verá a seguir, despertou a consciência de que um enfoque feito exclusivamente através do direito interno não era suficientemente eficaz, dado que a coleta e tratamento de dados pessoais pode facilmente ser feito fora dos confins de um Estado, razão pela qual se optou por uma uniformização normativa (DONEDA, 2006, p. 229). Ademais, seu conjunto constitui "[...] um patrimônio que formou a doutrina sobre proteção de dados pessoais que hoje se apresenta como disciplina jurídica dotada de autonomia.". (DONEDA, 2015, p. 371).

O surgimento dessas legislações foi impulsionado pelo contexto generalizado do Estado social, que para o funcionamento de sua burocracia e para fins de planejamento, exigia a coleta e processamento dos dados dos cidadãos. Tanto no contexto americano, como no europeu, na década de 1960, surgiram iniciativas dos Estados de, diante da chegada do aparato tecnológico

[30] Sobre a diferença entre diretiva e regulamento: "Um «Regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE, não carecendo de transposição para a ordem jurídica nacional. Tem um caráter geral e é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros (art. 288.º do Tratado sobre o Funcionamento da União Europeia). Uma directiva é um ato legislativo que fixa um objetivo geral que todos os países da EU devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo (art. 288.º do Tratado sobre o Funcionamento da União Europeia).". (FERREIRA, 2018, p. 23-24).

[31] Fortes (2016, p. 129-132) identifica oito instrumentos normativos que tratam da proteção de dados pessoais: 1) A *Health Insurance Portability and Accountability Act of 1996* (regula o uso e divulgaçãi de informações de saúde protegidas; 2) a *Gramm-Leach-bliley Act* ou *Financial Services Modernization of 1999* (exigem que instituições financeiras expliquem a seus cliente duas práticas de compartilhamento de informações e de proteção de dos dados confidenciais e sensíveis); 3) O *Fair Credit Reporting Act* (regula a coleta, a divulgação e o uso de informações do consumidor, incluindo informações de credito ao consumidor; 4) O *Fair Debt COllection Practies Act* (forma a base dos direitos de crédito ao consumidor nos Estados Unidos, aprovada em 1970; 5) A *Freedom od Information Act of 1996* (Lei de Liberdade de Informação dos Estados Unidos); 6) A *Privacy Act 1974* (regula a coleta, manutenção, utilização e divulgação de informações sobre indivíduos, mantidas em sistemas de registros por agências federais); 7) A *Elenctronic Communications Privacy Act* (regula a interceptação de conversas telefônicas) e suas atualizações; e, 8) A *USA PAtriot Act of 2001* (relacionadas ao combate ao terrorismo em reação aos atentados de 11 de setembro de 2001).

e sua capacidade de armazenamento e tratamento estatístico, possuírem legalmente uma grande base de dados. Exemplos são a "National Data Center" nos EUA e o projeto francês denominado "Sistema automatizado para o fichamento administrativo e o repertório dos indivíduos" (SAFARI), cujos debates na esfera pública e nos respectivos poderes legislativos alertaram os potenciais danos que tal centralização de dados poderia causar (MENDES, 2008, p. 30).

Destes debates surgiram as primeiras leis de proteção de dados, na década de 1970. São elas a lei alemã de 1970, a primeira lei de proteção de dados sueca que foi o Estatuto para bancos de dados de 1973, e, a *Privacy Act* norte americana de 1974 (DONEDA, 2015, p. 371). Estas leis tinham preocupação com os bancos de dados e não se falava em direitos dos cidadãos e instrumentos para garanti-los.

> A primeira destas quatro gerações de leis era composta por normas que refletiam o Estado da tecnologia e a visão do jurista à época, protendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo destas leis girava em torno da concessão de autorizações para a criação destes bancos de dados e do seu controle *a posteriori* por órgãos públicos. Estas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) destas normas. (DONEDA, 2015, p. 371).

A maioria das leis de proteção de dados de primeira geração buscava controlar o funcionamento dos bancos de dados através de licenças prévias e registros nos órgãos competentes. Conforme refere Bioni (2019, p. 114), "Temia-se a emergência da figura *orwelliana* do Grande Irmão, que poderia sufocar a liberdade do cidadão com uma vigilância ostensiva. Optou-se, então, por controlar a criação desses bancos de dados por meio da concessão de autorizações para o seu funcionamento.". Mas, a construção de grandes bancos de dados centralizados não se concretizou não apenas pela reivindicação dos cidadãos, como também pelo desenvolvimento do processamento de dados eletrônicos de forma descentralizada por pequenas unidades administrativas estatais e pela iniciativa privada (MENDES, 2008, p. 35). Se anteriormente a preocupação centrava-se no "Grande Irmão", agora passa a também ater-se aos "Pequenos Irmãos" (BIONI, 2019, p. 115).

Ao se desenvolver tecnologias que permitiam o processamento de dados de forma descentralizada, transformou-se completamente o debate sobre a proteção de dados pessoais, ocasionando uma necessidade de alteração legislativa. Passou-se a entender ser melhor que os cidadãos lutassem pela preservação de sua privacidade a partir de direitos, protegidos inclusive constitucionalmente, caracterizando a segunda geração de leis de proteção de dados.

A segunda fase é menos rigorosa para a criação de cadastros e também mais preocupada com relação à tutela dos direitos fundamentais (Lei francesa de 1978) (DONEDA, 2015, p. 372). Também observa Doneda (2015, p. 373), que

> A proteção de dado é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa.

Nesta fase, começa-se a perceber que o fornecimento dos dados pelo cidadão não se relacionava apenas com o setor público, mas que tinha se tornado condição indispensável para a vida em sociedade. Sua característica principal é a possibilidade de participação do indivíduo no processo de coleta e de processamento de dados através do seu consentimento. Nota-se que a estratégia regulatória da primeira geração era incumbir ao Estado licenciar a criação e autorizar o funcionamento dos bancos de dados, enquanto na segunda geração transfere-se para o próprio titular dos dados a responsabilidade de protegê-los (BIONI, 2019, p. 115).

Outra mudança, a ser destacada é a ampliação dos poderes das autoridades administrativas encarregadas da proteção de dados, com a finalidade de garantir o direito à privacidade, investigando ofensas à proteção de dados pessoais, sendo instituições da qual o cidadão poderia se reportar em caso de violação de algum de seu direito individual à proteção de dados pessoais (MENDES, 2008, p. 36). São elas "[...] tanto mais necessárias com a diminuição do poder do indivíduo para a autorização ao processamento de seus dados [...]" (DONEDA, 2015, p. 373-374), pois é irreal a efetividade do consentimento do cidadão e o exercício de sua liberdade de escolha[32], eis que a não disponibilização pode acarretar sua exclusão social, adverte Mendes (2008, p. 36):

> Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro lado, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca do cadastro de suas informações pessoais.

[32] Igualmente, o consentimento apresenta outros problemas, como: "[...] i) o problema da eficácia do consentimento do indivíduo acarretar a sua exclusão do mercado de consumo e da sociedade; ii) o problema da violação da proteção de dados pessoais, após o tratamento ter sido consentido pelo titular dos dados; iii) a questão do consentimento aplicado ao tratamento dos dados sensíveis.". (MENDES, 2008, p. 50).

Tendo em vista a dificuldade das pessoas em exercer seus direitos à proteção de dados, houve a necessidade de uma nova geração de leis. A terceira geração de normas de proteção de dados se inicia com a decisão do Tribunal Constitucional alemão sobre a inconstitucionalidade da "Lei do censo", em 1983. Aprovada pelo parlamento alemão possibilitava a retificação de registro civil a partir dos seus dados, o que acabou gerando um debate público e também um boicote da população ao censo, informações que eram coletadas em todos os Estados para manejarem suas políticas públicas.

A diferença na decisão do Tribunal alemão em relação às normas anteriores de proteção de dados pessoais é a ampliação da participação do cidadão no processamento de seus dados em todo o processo, desde a coleta, armazenamento e a transmissão (MENDES, 2018, p. 37). Alcança-se assim, o "[...] o êxtase da própria terminologia da "autodeterminação informacional", pois, com tal participação, possibilitar-se-ia que o sujeito tivesse um controle mais extensivo sobre as suas informações pessoais [...]" (BIONI, 2019, p. 116), e, o papel do consentimento sendo quase como sinônimo da autodeterminação informacional questionado e reafirmado como o seu ponto central (BIONI, 2019, p. 117).

Outra consequência ao desenvolvimento destas iniciativas precursoras foi a consciência de que um enfoque no direito interno era ineficaz diante o fato de que a coleta e o tratamento de dados pessoais poderiam facilmente ser feito fora dos limites territoriais do Estado (DONEDA, 2006, p. 229). Ao mesmo tempo em que legislações nacionais foram lançadas, organizações internacionais também passaram a regular a matéria, tendo como destaque a Convenção do Conselho da Europa para a Proteção dos Indivíduos face ao Tratamento Informático de Dados Pessoais, também conhecida como Convenção de Estrasburgo (que não foi estruturada como uma convenção unicamente "europeia", tendo sido aberta para adesões também de países não-membros do Conselho da Europa) e as *Guidelines* da Organização Para a Cooperação e o Desenvolvimento Econômico (OCDE) de 1980 e 1981 (DONEDA, 2006, p. 230-231). Uma das condicionantes para que o indivíduo possa exercer o seu poder de autodeterminação informativa é a existência de princípios[33] que devem nortear o tratamento de dados pessoais. Doneda (2006, p. 216-217), elabora uma síntese destes princípios:

[33] "**Artigo 5º - Qualidade dos dados.** Os dados de carácter pessoal que sejam objeto de um tratamento automatizado devem ser: **a)** Obtidos e tratados de forma leal e lícita; **b)** Registados para finalidades determinadas e legítimas, não podendo ser utilizados de modo incompatível com essas finalidades; **c)** Adequados, pertinentes e não excessivos em relação às finalidades para as quais foram registados: **d)** Exatos e, se necessário, atualizados; **e)** Conservados de forma que permitam a identificação das pessoas a que respeitam por um período que não exceda o tempo necessário às finalidades determinantes do seu registo.". (CONSELHO DA EUROPA, 1981).

> 1 – *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos.
> 2 – *Princípio da exatidão:* Os dados armazenados deve ser fieis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade.
> 3 – *Princípio da finalidade,* pelo qual toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes de sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).
> 4 - *Princípio do livre acesso,* pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias destes registos com a consequente possibilidade de controle destes dados, após este acesso de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou ainda pode-se proceder a eventuais acréscimos.
> 5 – *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Estes princípios influenciam as demais leis posteriores de proteção de dados pessoais, sendo sua aplicação, diante da Convenção de Estrasburgo, o principal marco de uma abordagem da matéria pelo viés dos direitos fundamentais (DONEDA, 2015, p. 378). É também inserida na esfera dos direitos humanos, orientada em torno do artigo 8º da Convenção Europeia para os Direitos do Homem, resultado de uma análise do Conselho da Europa, em 1968, para descobrir até que ponto as leis dos países europeus poderiam defender seus cidadãos dos problemas causados pelas novas tecnologias (DONEDA, 2006, p. 231).

A quarta fase, marcada pela Diretiva 95/46/CE da União Europeia, procura possibilitar a livre circulação dos mesmos especialmente no âmbito da União Europeia (LIMBERGER, 2007, p. 79). Verifica-se a presença de dois eixos, de um lado a proteção da pessoa e de outro a necessidade de proporcionar a livre circulação de mercadorias, incluindo a utilização de dados pessoais (DONEDA, 2006, p. 237).

A quarta geração visou resolver alguns problemas das legislações anteriores, tornando sem custos as reclamações individuais a respeito da violação à proteção de dados pessoais, e também proibindo total ou parcialmente determinadas categorias de dados classificados como sensíveis, pois seu tratamento gerava um potencial de discriminação, como no caso dos dados relativos à etnia, opção sexual, opinião política e religião[34]. Segundo explica Bioni (2019, p.

[34] Artigo 6º da Convenção 108 do Conselho da Europa. Categorias especiais de dados. Os dados de carácter pessoal que revelem a origem racial, as opiniões políticas, as convicções religiosas ou outras, bem como os dados de carácter pessoal relativos à saúde ou à vida sexual, só poderão ser objeto de tratamento automatizado desde que o direito interno preveja garantias adequadas. O mesmo vale para os dados de carácter pessoal relativos a condenações penais. (CONSELHO DA EUROPA, 1981).

85), os dados sensíveis são um tipo diferente em razão de seu conteúdo oferecer uma vulnerabilidade a discriminação, em afronta ao princípio da igualdade.

A igualdade se apresenta como um princípio ameaçado diante da vigilância exercida pelo Estado e pelo mercado a partir das informações obtidas em bancos de dados "[...] que pode acarretar a classificação e a discriminação dos indivíduos, afetando expressivamente as suas oportunidades sociais.". (MENDES, 2008, p. 50). A proteção dos dados pessoais sensíveis é fundamental para o pleno exercício de outros direitos fundamentais como a liberdade e a privacidade[35] (MULHOLLAND, 2018, p. 168).

Em 07 de dezembro de 2000, o Parlamento Europeu proclama a Carta dos Direitos Fundamentais da União Europeia, e trata, no art. 7º, do respeito à vida privada[36], e, no art. 8º, da proteção de dados pessoais[37], reconhecendo a complexidade deste pelo envolvimento com outros direitos fundamentais (DONEDA, 2006, p. 27). Prevê, também, a existência de uma autoridade independente. A criação pelos Estados-membros de autoridades de controle independentes já era taxativa no considerando nº 62 como elemento fundamental para a proteção das pessoas e o tratamento dos dados pessoais (FORTES, 2016, p. 156-157). Para Rodotà (2008, p. 86), "O órgão de controle configura-se assim como uma instituição 'que completa' o sistema de proteção de dados.".

Observa-se que diferentemente da concepção liberal, entende-se que a privacidade, na sua vertente de proteção de dados pessoais ultrapassa a dimensão de um direito individual fundamental, exercendo um papel importante perante a sociedade, atingindo propósitos coletivos como a preservação da democracia (MENDES, 2008, p. 42). Fortes (2016, p. 156) ressalta o Tratado que propôs a criação de uma constituição com jurisdição nos países membros da União europeia traz no artigo I-51[38] a proteção de dados pessoais na seção da "Vida democrática da União".

---

[35] Bioni (2019, p. 86) ressalta o estudo da Universidade de Cambridge sobre as curtidas em uma rede social podem revelar muitos atributos da personalidade de um indivíduo, dentre os quais informações sensíveis a seu respeito. Como visto no primeiro capítulo através da análise da mutação do conceito de privacidade e o exemplo do escândalo Cambridge Analytica, e reforçado agora com o estudo da proteção dos dados sensíveis, "[...] a proteção de dados pessoais perpassa a própria tutela do princípio da isonomia, na medida em que é um instrumento de contenção às práticas discriminatórias.". (BIONI, 2019, p. 86).

[36] "*Artigo 7.º* **Respeito pela vida privada e familiar.** Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.". (UNIÃO EUROPEIA, 2000).

[37] "*Artigo 8.º* **Proteção de dados pessoais.** Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.". (UNIÃO EUROPEIA, 2000).

[38] Ver nota 24 e 29.

Portanto, existe um regime geral para a coleta de dados[39], regulado através do princípio do consentimento do titular dos dados pessoais[40] para que sejam usados e circulados (GONÇALVES, 2003, p. 174), permitindo ajustar os interesses de autonomia da vontade, a circulação de dados e dos direitos fundamentais (DONEDA, 2005, p. 371). A autodeterminação informativa ou informacional, baseada no consentimento, é um modelo replicado na União Europeia, Canadá e Argentina, tendo como base a OCDE e a *Fair Information Pratices principles* (FIPPs) (BIONI; LIMA, 2015, p. 268). Este parâmetro normativo, objetiva "[...] haver a ciência do usuário, seguida de sua escolha em permitir ou barrar a coleta, tratamento, uso e transmissão dos dados pessoais, sob pena de tal prática ser ilícita.". (BIONI; LIMA, 2015, p. 268).

Porém, a Comissão Europeia, em 2009, percebeu que em decorrência do rápido avanço tecnológico era necessário alterar a regulamentação existente. Neste sentido, ressalta Magrani (2019, p. 119):

> Desta forma, iniciou estudos que se focavam (i) nos impactos das novas tecnologias; (ii) na falta de harmonia entre os Estados-Membros; (iii) na globalização e na internacionalização das transferências de dados; (iv) na necessidade de garantir cumprimento efetivo; e (v) na menor fragmentação dos instrumentos. O GDPR foi proposto em 2012 pela Comissão Europeia e seguiram quatro anos de intensas negociações entre o Parlamento Europeu e o Conselho da União Europeia, até que, em abril de 2016, a versão final foi publicada.

Após estas discussões na Europa, foi aprovado o Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679), aplicável desde 25 de maio de 2018, substituindo a Diretiva de Proteção de Dados de 1995 (95/46/CE), com a finalidade de revisar a legislação europeia acerca do assunto. É aplicável a todos os 28 países da União Europeia, incluindo

[39] Na linha das gerações de leis de proteção de dados, importante observar, como refere Fortes (2016, p. 162), a Diretiva 2002/58/CE, editada no ano de 2002, com o objetivo de harmonização das relações entre os países-membros e na garantia da proteção do direito à privacidade e ao tratamento adequado de dados pessoais, no âmbito das comunicações eletrônicas, assegurando a livre circulação desses dados e de equipamentos e serviços de comunicações eletrônicas na circunscrição europeia.

[40] Há também regimes próprios, como em relação aos dados sensíveis. "Artigo 8º. Tratamento de certas categorias específicas de dados. 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.". (UNIÃO EUROPEIA, 1995).

mudanças que incluem uma nova Diretiva de Proteção de Dados para os setores de polícia[41] e justiça criminal[42].

Umas das mudanças do Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) consistem no fato de que as empresas que oferecem bens e serviços na União Europeia que lidem com o tratamento de dados pessoais de pessoas residentes no seu território, devem demonstrar claramente que podem processar estes dados[43], comprovando o consentimento do usuário[44].

> Do ponto de vista operacional, a exigência de ter de comprovar a conformidade com o regulamento muda a forma de encarar a problemática da proteção de dados dentro das organizações. Até maio de 2018, a proteção de dados foi regulada numa perspectiva de hetero-regulação, em que a necessidade de garantir a licitude do tratamento, através dos princípios e condições de legitimidade, ocorria essencialmente na fase inicial, pelos meios definidos pela autoridade de controle (notificação, uma licença ou autorização, por exemplo). Após a entrada em aplicação do RGPD, estamos perante uma nova realidade. O responsável pelo tratamento tem que conseguir, em qualquer momento do processo de tratamento de dados pessoais, a sua licitude e cumprimento com o RGPD, criando evidências para que o possa comprovar, ficando assim sujeito à fiscalização e supervisão da autoridade de controle [...]. (FERREIRA, 2018, p. 62-63).

---

[41] "DIRETIVA 2016/281 (EU) DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativa à utilização dos dados dos registros de identificação dos passageiros (PNR) para efeitos de prevenção, detecção, investigação e repressão das infrações terroristas e da criminalidade grave.". (UNIÃO EUROPEIA, 2016c).

[42] "DIRETIVA 2016/280 (EU) DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão Quadro 2008/977/JAI do Conselho.". (UNIÃO EUROPEIA, 2016b).

[43] "Artigo 5.o. Princípios relativos ao tratamento de dados pessoais. 1. Os dados pessoais são: a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»); b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («limitação das finalidades»); c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»); d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»); e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»); f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»); 2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («responsabilidade»). (UNIÃO EUROPEIA, 2016a).

[44] A regra é que o tratamento de dados ocorra somente com o consentimento do titular, havendo hipóteses de exceção (artigo 6º), que preveem o tratamento sem o consentimento. "Artigo 7.o. Condições aplicáveis ao consentimento. 1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.". (UNIÃO EUROPEIA, 2016a).

De outro lado, a nova regulação da União Europeia prevê direitos aos usuários[45], obrigações aos controladores e operadores de dados, revisam regras sobre transferência internacional de dados, estabelece multas, cria um regime regulatório transfronteiriço para a União Europeia, assim como positiva novos direitos aos usuários[46], dentre eles o direito de acesso, o direito à portabilidade de dados e o direito ao esquecimento (MAGRANI, 2019, p. 119).

O referido regulamento é estruturado em 11 capítulos: 1) disposições gerais; 2) princípios; 3) direitos do titular dos dados; 4) responsável pelo tratamento e subcontratante; 5) transferência de dados pessoais para países terceiros ou organizações internacionais; 6) autoridades de controlo independentes; 7) cooperação e coerência; 8) vias de recurso, responsabilidade e sanções; 9) disposições relativas e situações específicas de tratamento; 10) atos delegados e atos de execução; e, 11) disposições finais.

Os elementos do modelo europeu, portanto, decorrem da Convenção de Estrasburgo (Convenção 108 do Conselho da Europa para a Proteção dos Indivíduos face ao Tratamento Informático de Dados Pessoais de 1981), definindo a proteção de dados como um direito humano e um direito fundamental, no que se depreende do artigo 8º da Convenção Europeia de Direitos do Homem. A Diretiva de Proteção de Dados de 1995 (95/46/CE), e posterior Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679), se baseiam em dois princípios básicos, definido no artigo 1º, a de proteger direitos fundamentais, e a de facilitar a circulação dos dados dentro da União europeia[47]. Estabelecem princípios, limites e exceções ao tratamento de dados privados, como os dados sensíveis por exemplo, e estimulam o fluxo entre fronteiras, desde que tenha um nível de proteção de dados pessoais adequado ao padrão europeu (DONEDA, 2006, p. 238).

---

[45] Os direitos do titular estão previstos no Regulamento Geral de Proteção de Dados da União Europeia entre os artigos 12 a 23, dentre os quais: a) transparência e regras para o exercício dos direitos dos titulares dos dados (artigo 12º); b) informação e acesso aos dados pessoais (artigo 13º ao 15º); c) retificação e apagamento (artigo 13º ao 20º, dentre os quais o novo direito de portabilidade dos dados); d) direito de oposição e decisões individuais automatizadas (artigo 21º ao 22º); e) limitações (artigo 23º) (UNIÃO EUROPEIA, 2016a).

[46] Dentro os quais pode-se destacar o direito a portabilidade dos dados, que implica em conceder ao interessado a possibilidade de recuperação e transferência de seus dados para outra entidade responsável, e o direito a não ser submetido a uma decisão exclusivamente automatizada, por exemplo, em perfis destinados a avaliar determinados aspectos da personalidade, tais como rendimento laboral, crédito, conduta, gostos. (PROVIEW, 2018, p. 36-37).

[47] "Disposições gerais. Artigo 1.o. Objeto e objetivos. 1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais. 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.". (UNIÃO EUROPEIA, 2016a).

A legislação União Europeia de proteção de direitos humanos reconhece possíveis colisões como a proteção de dados e o direito à informação. Deste modo, há também a necessidade de se privilegiar um modelo jurídico de reconhecimento de fontes de legitimidade exteriores ao sistema político do Estado, com modalidades de tutela da proteção de dados que exigem a utilização de mecanismos de auto-regulamentação e de meios técnicos (DONEDA, 2006, p. 362).

É o caso da "Privacy by Default"[48], e a segurança dos dados, como a anonimização, a notificação de invasão da base de dados e auditorias [49]. Ferreira (2018, p. 62-63) aduz que contrariando o que seria recomendável e nas raras vezes em que as organizações já tinham precauções com o procedimento de proteção de dados, as respostas vinham após incidentes de violação de dados ou de sanções da autoridade de controle. Trata-se de um novo paradigma, cujo objetivo é "[...] encarar estas medidas de proteção de dados desde a concepção e por pré-definição, como pressupostos do desenho do sistema a implementar. O sentido [...] é o de revelar uma visão preventiva e não uma visão com recurso a medidas avulsas, reativas ou improvisadas.". (FERREIRA, 2018, p. 62-63).

Por isso, além do paradigma do consentimento nas leis de proteção de dados na União Europeia, é possível observar juntamente a emergência de um novo paradigma normativo, o da regulação do risco. O regime de regulação de risco adotado na proteção de dados depende especialmente do caráter regulador da autoridade de proteção de dados (ZANATTA, 2017). Ainda, saídas não essencialmente jurídicas, como *standarts*, códigos de ética, segurança dos dados através da anonimização[50] e da criptografia, e mesmo legitimidade de organizações da sociedade civil como a academia e organizações não governamentais para fiscalizar e instrumentalizar estes direitos servem como verdadeiras barreiras para o avanço tecnológico desenfreado (ZANATTA, 2017). Conforme Mendes (2018, p. 1-2):

---

[48] "Artigo 25.o. Proteção de dados desde a concepção e por defeito. 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.". (UNIÃO EUROPEIA, 2016a).

[49] Artigo 32º (Segurança do tratamento), Artigo 33º (Notificação de uma violação de dados pessoais à autoridade de controle), Artigo 34º (Comunicação de uma violação de dados pessoais ao titular dos dados), Artigo 35º e Artigo 36º, Avaliação de impacto sobre a proteção de dados e consulta prévia. (UNIÃO EUROPEIA, 2016a).

[50] "*Artigo 4.º* **Definições.** Para efeitos do presente regulamento, entende-se por: "[...] 5) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável; [...]" (UNIÃO EUROPEIA, 2016a).

> O intenso processamento de dados pelos setores públicos e privado a partir da década de 1970 ensejou a evolução do direito à privacidade, abarcando uma dimensão de proteção de dados pessoais, com destaque para o controle do indivíduo sobre o fluxo de suas informações na sociedade. Já a geração de normas de proteção de dados que começa a se desenvolver agora é amparada no princípio da *accountability*. Entende-se que a efetividade da proteção de dados não decorre apenas da ampliação do controle do indivíduo, mas inclui também a atribuição de responsabilidade a toda a cadeia de agentes de tratamento de dados pelos riscos do processamento de informações, uma vez que esses agentes têm mais condições de implementar medidas técnicas e organizativas capazes de proteger os dados pessoais dos titulares.

Com a proteção de dados, aponta-se um processo de "risquificação" do direito, onde a afirmação de direitos fundamentais é complementada por uma preocupação maior com instrumentos *ex ante,* licenças, análises de risco, processos de documentação e *accoutability* por parte dos "controladores" e "processadores" de dados (ZANATTA, 2017). O modelo teórico regulatório da proteção de dados vem recebendo uma nova abordagem centrada na regulação do risco[51], e isto, "[...] provoca uma mudança de rota para a prevenção de danos *antes que eles ocorram* e instrumentos regulatórios que incrementem o nível de informação e cognição de riscos por autoridades especializadas, bem como um conjunto de obrigações às empresas de tecnologia [...]". (ZANATA, 2017, p. 188-189, grifo do autor.).

Em suma, diversas garantias fundamentais e direitos de personalidade vêm tendo seu perfil modificado há um bom tempo, por efeito ou diálogo direto com o desenvolvimento tecnológico. O debate, portanto, é sobre a melhor forma de adotar soluções que preservem os direitos humanos e direitos fundamentais. O Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) possui impacto internacional, exigindo atenção às diferenças e similitudes com as regulações nacionais.

O regime regulatório de transferência internacional de dados na legislação brasileira de proteção de dados, como será aprofundado no próximo subcapítulo, por exemplo, é por ele influenciado. Como já visto, o Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) possui aplicação direta em todos os Estados-Membros, tendo todos os países as mesmas regras e garantias de proteção de dados, o que possibilita um nível mais coerente e homogêneo nas atividades e meios de tratamento (FERREIRA, 2018, p. 40).

A necessidade de aplicação coercitiva das mesmas regras, pelos Estados, decorre das novas exigências tecnológicas, a demonstrar que o marco regulatório de dados pessoais

[51] "A recomendação de 2010 do Conselho da Europa de que a perfilização pode levar a riscos significantes para as liberdade e direitos individuais, o relatório sobre aplicação dos princípios da Convenção 108 sobre coleta e processamento de dados biométricos apontando a necessidade de aplicação do princípio da precaução, que seria um princípio inerente a regulação de risco, a existência de autoridade com alta expertise técnica e na criação de obrigações de produção de informação sobre riscos ao setor privado como estudos de impacto à privacidade." (ZANATA, 2017).

anteriormente aplicado na União Europeia, em que a concentração do controle sobre os dados pessoais centrava-se no próprio cidadão se demonstrou não muito eficiente, pois muitas vezes as consequências do tratamento de dados escapavam a sua compreensão, passando-se a entender que a proteção dos direitos fundamentais em jogo exigia uma atuação positiva do Estado, promovendo a tutela dos dados pessoais. Portanto, a criação de autoridade de controle nos Estados-membros, habilitados a desempenhar as suas funções e a exercer os seus poderes com total independência constitui um elemento essencial da proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais (Consideração número 117 do Regulamento Geral de Proteção de Dados).

Alguns autores, como Doneda (2006) e Limberger (2007), procuram demonstrar que a origem das autoridades de proteção de dados está nas agências reguladoras independentes e no debate sobre a teoria da regulação (INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, 2019). Em uma concepção mais tradicional e jurídica sobre o termo *regulação,* centrado no Estado, incluem-se legislação, licenças, códigos, normas, atos administrativos e suas agências públicas. Neste sentido, Zanata (2015, p. 450) anota

> Na autorregulação, o setor privado se organiza e cria "*standards*" e normas procedimentais para a conduta dos atores, independentemente do Estado. Em termos gerais, é o que ocorre na regulação da propaganda (Conar) e da Bolsa de Valores (Bovespa). Na "corregulação", o Estado reconhece a importância da produção espontânea de normas pelo setor privado, mas monitora e valida tais normas. Por fim, o tipo da "regulação tradicional" consiste na criação de regras e comandos mediante ameaça de sanções (sanções penais ou multas administrativas). (ZANATA, 2015, p. 450).

Pode-se apontar que na proteção de dados há a corregulação na proteção de dados pessoais, diante da exigência de uma lei geral para o tema, na qual também há a valorização da autonomia do titular dos dados, e a existência de uma autoridade de proteção. Para Silva (2012, p. 309), essa forma de regulação "[...] ao mesmo tempo em que valoriza a participação social e política dos usuários, vinculando os particulares à defesa de direitos fundamentais, também salvaguarda os espaços de liberdade em face do Estado [...]".

Ao contrário das agências reguladoras independentes, que regulam mercados ou setores de serviços públicos, as autoridades de proteção de dados têm como traço distintivo a atribuição de zelar pelo tratamento de dados pelos atores privados e públicos, e, em razão disto, sua independência se torna ainda mais fundamental. Por outro lado, há pouca pesquisa sobre autoridade de proteção de dados e os fundamentos das agências regulatórias independentes fornece uma estrutura para a análise de seu conceito de independência (SCHUTZ, 2011).

> Há políticas públicas que, por características de fato e de direito, podem ser formuladas, implementadas, fiscalizadas e avaliadas pela própria administração direta, de forma mais ou menos descentralizada. Algumas políticas sociais ou boa parte da política educacional e de saúde, por exemplo, umbilicalmente ligadas à razão de ser estruturas estatais, exemplificam a opção (em alguns casos, por mandamento constitucional, a obrigação). Há outras, cujos atributos – falta de competitividade no setor, necessidade de desconcentração, necessidade de alta especialização técnica, proteção frequente a eventuais inflexões políticas, rápida mutação e consequente exigência de atuação mais ágil etc. – recomendam arranjos institucionais distintos. A existência de entidades autônomas independentes tanto no mérito de suas decisões quanto em sua gestão administrativo-financeira, com corpo burocrático técnico e especializado, e com bom grau de abertura à participação de atores relevantes ao processo, coloca-se como uma das alternativas possíveis. (VASCONCELOS, PAULA, 2019, p. 721-722).

Conforme já visto sobre as Autoridades Nacionais de Proteção de Dados, quando abordado sua criação como novo procedimento exigido pelos direitos de terceira geração de que trata Pérez Luño, as suas principais funções são de execução de políticas de privacidade e conscientização da população, sendo fundamental a independência do mercado e do domínio político. Sua relação com as agências reguladoras consiste na independência deste modelo institucional como elemento importante de sua legitimidade pela "[...] percepção de uma maior especificidade técnica de seus funcionários e do comprometimento com a continuidade de políticas nos setores regulados, já que não estariam diretamente sujeitas às trocas de partidos políticos no governo.". (INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, 2019, p. 06).

As entidades reguladoras possuem uma série de poderes conferidos para a sua independência e autonomia técnica e administrativa. Eles abrangem os clássicos poderes administrativos do Estado, e outros como a fiscalização de atividades e o "[...] cumprimento das regras estabelecidas nos contratos de concessão, nas licenças ou nas autorizações incluindo o estabelecimento de eventuais tarifas, poderes disciplinares sancionatórios e preventivos de condutas prejudiciais aos interesses coletivos tutelados, etc.". (ARAGÃO, 2000, p. 280).

A importância da Autoridade Nacional de Proteção de Dados para a aplicação das leis de proteção se constatou desde suas primeiras gerações, nos anos 1960, na União Europeia (LUCCA, LIMA, 2020, p. 377). As autoridades de proteção de dados são uma parte crucial na arquitetura de direitos fundamentais da União Europeia. Atualmente, pode-se dizer que grande parte das Autoridades Independentes de Proteção de Dados dos países europeus atualizaram suas legislações em razão do Regulamento Geral de Proteção de Dados da União Europeia.

O Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679), em seu capítulo sexto, trata das autoridades de proteção de dados, denominadas como Autoridades de

Controle Independentes, constantes entre os artigos 51 ao 59. É subdividida em duas secções, uma que trata de sua independência e outra sobre a competência, atribuições e poderes.

Os Estados-Membros estabelecem que cabe a uma ou mais[52] autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União (artigo 51). São lhe assegurados independência e autonomia técnica e financeira[53] para exercer suas funções.

O regulamento estabelece as condições gerais aplicáveis aos membros da autoridade de controle (artigo 53), sendo basicamente que eles sejam nomeados por procedimento transparente pelo Parlamento, Governo, Chefe de Estado, ou, um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro, e que possuam habilitações, experiência e conhecimentos técnicos necessários no domínio da proteção de dados pessoais. E ainda, a garantia de exoneração somente ao final do mandato ou por cometimento de falta grave ou descumprimento das condições exigidas para o exercício das suas funções.

Já o artigo 54 prevê as regras aplicáveis à constituição da autoridade de controle. Os Estados-Membros estabelecem, por via legislativa, sua constituição, a qualificação e condições de elegibilidade necessárias para a nomeação dos seus membros e suas as regras e os procedimentos de nomeação, a duração do mandato observando sempre a independência. Por sua vez, o artigo 55 trata da competência das autoridades de controle, sendo elas executar as atribuições e exercer os poderes que lhe são conferidos pelo regulamento no território do seu próprio Estado-Membro. O artigo 56 trata ainda de definição de competência em casos em razão do local do estabelecimento principal do responsável pelo tratamento ou do subcontratante.

---

[52] Para a defesa no Brasil de um modelo de autoridade local de proteção de dados pessoais, ver Bolesina (2016) em sua tese intitulada "O direito à extimidade e a sua tutela por uma autoridade local de proteção de dados pessoais: as inter-relações entre identidade, ciberespaço, privacidade e proteção de dados pessoais em face das intersecções jurídicas entre o público e o privado.", sendo que a previsão do Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) permite a formatação pleiteada, tal como ocorre na Alemanha (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 19)

[53] "*Artigo 52.º*. **Independência.** 1. As autoridades de controlo agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do presente regulamento. 2. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem. 3. Os membros da autoridade de controlo abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível. 4. Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comité. 5. Os Estados-Membros asseguram que cada autoridade de controlo selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controlo interessada. 6. Os Estados-Membros asseguram que cada autoridade de controlo fique sujeita a um controlo financeiro que não afeta a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional.". (UNIÃO EUROPEIA, 2016a).

As atribuições[54] das autoridades de proteção de dados decorrem de sua responsabilidade pela fiscalização e cumprimento do regulamento. Se revela não menos importante assegurar que ao conhecimento público das normas que regulam a matéria (RODOTÀ, 2008, p. 253), bem como, conforme texto legal, promover a sensibilização e compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento de seus dados pessoais.

As autoridades de proteção de dados também devem dispor de poderes consultivos na elaboração de medidas legislativas e administrativas ou regulamentos relativos à proteção de dados, de fornecer aconselhamento e informação a particulares envolvidos em operações de tratamento de dados e emitir normas setoriais. Também devem se envolver em uma série de atividades direcionadas à avaliação do sistema de proteção de dados e em disseminar sua cultura (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 28).

---

[54] "*Artigo 57.º*. **Atribuições.** Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controlo, no território respectivo: a) Controla e executa a aplicação do presente regulamento; b) Promove a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial; c) Aconselha, em conformidade com o direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento; d) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento; e) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito; f) Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.o, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo; g) Coopera, incluindo partilhando informações e prestando assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento; h) Conduz investigações sobre a aplicação do presente regulamento, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública; i) Acompanha fatos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações e das práticas comerciais; j) Adota as cláusulas contratuais-tipo previstas no artigo 28.o, n.o 8, e no artigo 46.o, n.o 2, alínea d); k) Elabora e conserva uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35.o, n.o 4; l) Dá orientações sobre as operações de tratamento previstas no artigo 36.o, n.o 2; m) Incentiva a elaboração de códigos de conduta nos termos do artigo 40º, nº 1, dá parecer sobre eles e aprova os que preveem garantias suficientes, nos termos do artigo 40.º, nº 5; n) Incentiva o estabelecimento de procedimentos de certificação de proteção de dados, e de selos e marcas de proteção de dados, nos termos do artigo 42.o, n.o 1, e aprova os critérios de certificação nos termos do artigo 42.o, n.o 5; o) Se necessário, proceder a uma revisão periódica das certificações emitidas, nos termos do artigo 42.o, n.o 7; p) Redige e publicar os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43; q) Conduz o processo de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.o e de um organismo de certificação nos termos do artigo 43.o ; r) Autoriza as cláusulas contratuais e disposições previstas no artigo 46.o, n.o 3; s) Aprova as regras vinculativas aplicáveis às empresas nos termos do artigo 47.o , t) Contribui para as atividades do Comité; u) Conserva registos internos de violações do presente regulamento e das medidas tomadas nos termos do artigo 58.o, n.o 2; e, v) Desempenha quaisquer outras tarefas relacionadas com a proteção de dados pessoais." (UNIÃO EUROPEIA, 2016ª).

Em relação aos poderes[55] das autoridades de proteção de dados, podem ser divididos em poderes de investigação, poderes de correção, poderes consultivos e de autorização, sendo indispensáveis na execução de suas tarefas. As autoridades de proteção de dados devem ser dotadas de poderes de investigação, como o poder de acesso aos dados e informações necessárias para o desempenho de suas funções de supervisão. Deve também ser dotado com poderes de intervenção, como o de emitir pareceres antes das operações de processamento de dados sensíveis serem realizadas e garantir a publicação adequada desses pareceres, ordenar o bloqueio, apagamento e destruição de dados, proibir temporária ou definitivamente o

[55] "*Artigo 58.o*. **Poderes.** 1. Cada autoridade de controlo dispõe dos seguintes poderes de investigação: a) Ordenar que o responsável pelo tratamento e o subcontratante e, se existir, o seu representante, lhe forneçam as informações de que necessite para o desempenho das suas funções; b) Realizar investigações sob a forma de auditorias sobre a proteção de dados; c) Rever as certificações emitidas nos termos do artigo 42.o, n.o 7; d) Notificar o responsável pelo tratamento ou o subcontratante de alegadas violações do presente regulamento; e) Obter, da parte do responsável pelo tratamento e do subcontratante, acesso a todos os dados pessoais e a todas as informações necessárias ao exercício das suas funções; f) Obter acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União ou dos Estados-Membros. 2. Cada autoridade de controlo dispõe dos seguintes poderes de correção: a) Fazer advertências ao responsável pelo tratamento ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento; b) Fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento; c) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento; d) Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado; e) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais; f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição; g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16.o, 17.o e 18.o, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17.o, n.o 2, e do artigo 19.o; h) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42.o e 43.o, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos; i) Impor uma coima nos termos do artigo 83.o, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso; j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais. 3. Cada autoridade de controlo dispõe dos seguintes poderes consultivos e de autorização: a) Aconselhar o responsável pelo tratamento, pelo procedimento de consulta prévia referido no artigo 36.o; b) Emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao Parlamento nacional, ao Governo do Estado-Membro ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais; c) Autorizar o tratamento previsto no artigo 36.o, n.o 5, se a lei do Estado-Membro exigir tal autorização prévia; d) Emitir pareceres e aprovar projetos de códigos de conduta nos termos do artigo 40.o, n.o 5; e) Acreditar organismos de certificação nos termos do artigo 43.o; f) Emitir certificações e aprovar os critérios de certificação nos termos do artigo 42.o, n.o 5; g) Adotar as cláusulas-tipo de proteção de dados previstas no artigo 28.o, n.o 8, e no artigo 46.o, n.o 2, alínea d); h) Autorizar as cláusulas contratuais previstas no artigo 46.o, n.o 3, alínea a); i) Autorizar os acordos administrativos previstos no artigo 46.o, n.o 3, alínea b); j) Aprovar as regras vinculativas aplicáveis às empresas nos termos do artigo 47.o. 4. O exercício dos poderes conferidos à autoridade de controlo nos termos do presente artigo está sujeito a garantias adequadas, que incluem o direito à ação judicial efetiva e a um processo equitativo, previstas no direito da União e dos Estados-Membros, em conformidade com a Carta. 5. Os Estados-Membros estabelecem por lei que as suas autoridades de controlo estão habilitadas a levar as violações do presente regulamento ao conhecimento das autoridades judiciais e, se necessário, a intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições do presente regulamento. 6. Os Estados-Membros podem estabelecer por lei que as suas autoridades de controlo terão outros poderes para além dos previstos nos n.os 1, 2 e 3. O exercício desses poderes não deve prejudicar o efetivo funcionamento do capítulo VII.". (UNIÃO EUROPEIA, 2016a).

tratamento, emitir aviso e advertência ao controlador, além de serem notificados para que verifiquem previamente operações de tratamento de dados susceptíveis de apresentar riscos aos direitos e liberdades dos titulares dos dados.

Há de se destacar ainda, no sistema de proteção de dados europeu, que no ano de 2004, foi criada a Autoridade Europeia de Proteção de Dados, com sede em Bruxelas, através do Regulamento 45/2001. Mais recentemente houve uma atualização, diante do Regulamento Geral de Proteção de Dados, pelo Regulamento 2018/1725 do Parlamento Europeu e do Conselho [56]. Suas funções basicamente consistem em zelar pelo cumprimento das regras de privacidade que regem atividades de instituições e organismos da União Europeia que realizem o tratamento de dados pessoais dos cidadãos. Além de poderes de investigação de correção, de autorização e consultivos típicos das suas funções, a Autoridade Europeia de Proteção de Dados possui atribuições[57] que se complementam com as funções e atribuições da Autoridade Nacional de Proteção de Dados de cada país previstas no regulamento.

Conforme estudo da Agência de Direitos Fundamentais de União Europeia, no ano de 2010, ou seja, antes da aprovação do Regulamento Geral de Proteção de Dados, cada país possuía graus de independência distintos entre si, como por exemplo, na forma de escolha de

[56] "Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n. º. 45/2001 e a Decisão n.º 1247/2002/CE.[...]." (UNIÃO EUROPEIA, 2018).

[57] "Artigo 57.o. Atribuições. 1. Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, a Autoridade Europeia para a Proteção de Dados: a) Controla e garante a aplicação do presente regulamento pelas instituições e pelos órgãos da União, com exceção do tratamento de dados pessoais pelo Tribunal de Justiça no exercício das suas funções jurisdicionais; b) Promove a sensibilização do público e a sua compreensão dos riscos, das regras, das garantias e dos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser objeto de especial atenção; c) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento; d) Se lhe for solicitado, presta informações aos titulares dos dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades nacionais de controlo para esse efeito; e) Trata as reclamações apresentadas pelos titulares dos dados ou por organismos, organizações ou associações nos termos do artigo 67.o, investiga, na medida do necessário, o conteúdo das reclamações, e informa os seus autores do andamento e do resultado das investigações num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outras autoridades de controlo; f) Realiza investigações sobre a aplicação do presente regulamento, nomeadamente com base em informações recebidas de outras autoridades de controlo ou de outras autoridades públicas; g) Presta aconselhamento, por iniciativa própria ou mediante pedido, a todas as instituições e órgãos da União sobre medidas legislativas e administrativas relacionadas com a proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais; h) Acompanha factos novos relevantes, na medida em que tenham incidência na proteção dos dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações; i) Adota as cláusulas contratuais-tipo previstas no artigo 29.o, n.o 8, e no artigo 48.o, n.o 2, alínea c); j) Estabelece e conserva uma lista relativamente ao requisito de avaliação de impacto relativa à proteção de dados, nos termos do artigo 39.o, n.o 4; k) Participa nas atividades do Comité Europeu para a Proteção de Dados; l) Assegura o secretariado do Comité Europeu para a Proteção de Dados, nos termos do artigo 75.o do Regulamento (UE) 2016/679; m) Presta aconselhamento sobre o tratamento a que se refere o artigo 40.o, n.o 2; n) Autoriza as cláusulas contratuais e as disposições referidas no artigo 48.o, n.o 3; o) Conserva registos internos das violações do presente regulamento e das medidas tomadas nos termos do artigo 58.o, n.o 2; p) Executa outras tarefas relacionadas com a proteção de dados pessoais; e q) Elabora o seu regulamento interno. (UNIÃO EUROPEIA, 2018d).

seus diretores. No mesmo sentido, em relação aos recursos técnicos, este estudo apontava que alguns países de União Europeia apresentavam dificuldades de falta de financiamento, assim como, em alguns casos, as autoridades eram capazes de aumentar seus recursos financeiros através de receitas obtidas das notificações e sanções impostas (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 21-22).

A independência das autoridades de proteção de dados, garantida pela autonomia técnica e financeira é um fator essencial, pois, a ausência de recursos ameaça a proteção dos direitos fundamentais dos titulares dos dados (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 21-22). Um dos fatores que podem contribuir para o aprimoramento da autonomia do órgão de fiscalização é a sua inclusão no texto constitucional, como ocorre em Portugal, por exemplo (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 22).

Mas, os estudos sobre autoridades de proteção de dados envolvem além de pesquisa documental de leis, regulamentos e normas que os países europeus. Em infográfico apresentado pela Comissão Europeia (2019), abordando a implementação do Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679) após 01 (um) ano de sua entrada em vigor, na data de 25 de maio de 2018, consta que 67 % (sessenta e sete por cento) dos europeus já ouviram falar do Regulamento Geral de Proteção de dados da União Europeia. Em relação à autoridade de proteção de dados, 57% (cinquenta e sete por cento) dos europeus sabem que existe uma autoridade pública responsável por proteger os seus direitos sobre dados pessoais no seu país, e 20 % (vinte por cento) sabem qual autoridade pública é responsável. Desde maio de 2018, 144.376 (cento e quarenta e quatro mil e trezentos e setenta e seis) reclamações e consultas, e 89.271 (oitenta e nove mil e duzentos e setenta e um) notificações de violação de dados receberam todas as autoridades de proteção de dados na Europa.

Tendo em vista a influência deste modelo em países não pertencentes, também é preciso observar os modelos estrangeiros de autoridades de proteção de dados pessoais. Greenleaf (2017), apresenta um estudo sobre as autoridades de proteção de dados no mundo e suas redes globais, apontando que atualmente 120 (cento e vinte) países possuem leis de proteção de dados e que destes mais de 80 % (oitenta por cento) estão com suas autoridades independentes e especializadas em funcionamento. Coloca como países no "*Hall of Shame"* (Calçada da vergonha), aqueles países que legislando sobre a proteção de dados e nomeação de uma autoridade de proteção, o deixam de fazer por mais de um ano.

Um dos problemas técnicos identificados na pesquisa é a aplicação transfronteiriça[58] como uma probabilidade crescente de problemas a serem tratados por autoridades de proteção de dados, sendo desejável a existência de redes internacionais para facilitar a resolução de conflitos. No plano da organização de redes de autoridades de proteção, a Conferência Internacional dos Comissários de Proteção de Dados e Privacidade (ICDPPC) é a mais antiga, funcionando desde 1979, credenciando atualmente a maioria dos países que possuem autoridades de proteção de dados. No plano da representação de países, o maior agrupamento é o Comitê Consultivo da Convenção 108 do Conselho da Europa (GREENLEAF, 2017, p. 04).

A Conferência Internacional dos Comissários de Proteção de Dados e Privacidade (ICDPPC) também desenvolveu estudo (2017) sobre as autoridades de proteção de dados. Das 87 (oitenta e sete) autoridades existentes, mais da metade se estabeleceu depois da década de 2000. Outra informação que se destaca é que 98% (noventa e oito por cento) das autoridades estão presentes digitalmente e publicam relatórios anuais *on line.* Ainda, cerca de 85 % (oitenta e cinco por cento) dos países possuem referências constitucionais sobre a proteção de dados, bem como supervisionam os setores públicos e privados, e na maioria dos países conta-se com subsídios para o financiamento da autoridade, sendo uma pequena parte utiliza de multas e sanções.

Na União Europeia todos os países possuem uma autoridade de proteção de dados (GREENLEAF, 2017, p. 03). Em seus sítios eletrônicos é possível encontrar decisões sobre processos administrativos, normas setoriais e orientações sobre a proteção de dados e relatórios de suas atividades. O sistema de proteção de dados pessoais da Europa é bastante avançado, considerando seus países serem pioneiros em legislação sobre o tema, além de suas autoridades independentes de proteção de dados serem bastante atuantes, o que justifica que essas diretrizes sejam contrastadas com o tratamento normativo do tema no Brasil, que recentemente criou sua autoridade nacional de proteção de dados pessoais, conforme será desenvolvido a seguir.

[58] "O GDPR previu o sistema chamado *one-stop shop,* pilar central da nova regulação criada. Uma autoridade principal regula controladores de dados e, caso uma autoridade de supervisão conteste aquela, será dada uma decisão pelo Conselho Europeu de Proteção de Dados (EDPB na sigla em inglês), podendo haver apelação para a Corte de Justiça da União Europeia. [...] outra diretriz importante diz respeito à autoridade de supervisão que deve ser notificada pelos controladores em casos de violação de dados pessoais. Além disso, controladores e operadores devem designar um responsável pela proteção de dados (*Data Protection Officers – DPD),* cujas atividades principais consistem em regular e realizar sistemático monitoramento de dados pessoais ou do processamento de categorias especiais de dados em larga escala, conforme previsão do artigo 37 do GDPR.". (MAGRANI, 2019, p. 132-134).

3.2. A trajetória brasileira na Proteção de Dados Pessoais em perspectiva comparada: das promessas normativas para a atuação da autoridade nacional

No Brasil, até a edição da Lei Geral de proteção de dados (LGPD) em 2018, não existia uma regulamentação geral sobre o tema. O ordenamento jurídico brasileiro não se estruturava a partir de uma legislação unitária, mas de uma série de dispositivos decorrentes dos direitos de personalidade, como a liberdade de expressão e do direito à informação e o direito à privacidade (inviolabilidade da vida privada e intimidade) [59].

A Constituição Federal brasileira protege o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas[60]. Ainda, é possível visualizar o banco de dados no Código de Defesa do Consumidor, em dispositivos, por exemplo, que exigem a comunicação prévia ao afetado de um registro (art. 43, § 2º, do CDC) [61] e o Código Civil (art. 21) [62]. Ademais, pode-se relacionar a proteção de dados com o direito fundamental à igualdade[63], previsto no artigo 5º, *caput*, da Constituição Federal, e com os objetivos fundamentais da República Federativa do Brasil[64], constantes no artigo 3º. No entanto, como explica Doneda (2011, p. 104), até então pareceu,

> [...] existir no direito brasileiro, de forma generalizada, uma consciência de que seria possível tratar de forma satisfatória os problemas relacionados às informações pessoais em bancos de dados a partir de uma série de categorizações geralmente generalistas e algo abstratas: sobre o caráter rigidamente público ou particular de uma espécie de informação; a respeito da característica sigilosa ou não de determinada comunicação, e assim por diante. Enfim: com um sistema baseado em etiquetas, permissões ou proibições para o uso de informações específicas sem considerar os riscos objetivos potencializados pelo tratamento das informações pessoais.

[59] "X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial". (BRASIL, 1988).

[60] "XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.". (BRASIL, 1988).

[61] "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. [...] § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.". (BRASIL, 1990).

[62] "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.". (BRASIL, 2002).

[63] "Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes [...].". (BRASIL, 1988).

[64] "Art. 3º. Constituem objetivos fundamentais da República Federativa do Brasil: [...] IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação.". (BRASIL, 1988).

Por muito tempo, apenas existiu o *habeas data*[65], previsto no art. 5º, inciso LXXII, da Constituição Federal de 1988, concebido como um instrumento para ter acesso à informações sigilosas. No entanto, seu âmbito de proteção ainda era muito restrito[66], relacionado ao direito do cidadão de tomar conhecimento sobre as informações constantes em bancos de dados do Estado (LIMBERGER, 2007, p. 188-189). Mas, sua relevância decorre do contexto em que surge, em um regime político que não consagrava os direitos fundamentais.

A utilização *habeas data*, portanto, está relacionada a existência de uma pretensão resistida, quando houver uma recusa por parte do mantenedor do cadastro em responder ao pedido de acesso, retificação ou complementação das informações. Neste sentido, observa Mendes (2008, p. 121):

> O *habeas data* foi concebido como instrumento para possibilitar às vítimas do regime militar conhecerem arquivos e registros a seu respeito. Esse objetivo restrito que permeou o surgimento e o desenvolvimento do *habeas data* talvez tenha contribuído para a sua reduzida eficácia e utilização no ordenamento jurídico brasileiro. Ademais, outros fatores podem explicar a sua pouca utilização no país. Primeiramente, a sua redação não impõe qualquer limite ao armazenamento e ao tratamento de dados, pressupondo, portanto, que tais processos são legítimos *per se.* Segundo, tendo em vista que ele não prevê a possibilidade de exclusão de dados em bancos de dados, ele corrobora com o entendimento de que qualquer armazenamento e tratamento de dados é sempre legítimo. Pode-se dizer também que o seu caráter remedial, possibilitando o acesso aos dados apenas em caso da recusa do banco de dados em fazê-lo, relaciona-se a uma concepção muito liberal de privacidade, pouco condizente com a principiologia da Constituição federal.

As previsões legais a respeito da privacidade no ordenamento jurídico brasileiro, especialmente aquelas previstas na Constituição Federal, não se relacionam com um conceito mais amplo de privacidade, mas sim com um conceito mais liberal. Na Argentina, por exemplo, a regulamentação do *habeas data*, nos anos 2000, permitiu que fosse aprovada uma lei sobre a proteção de dados pessoais (Lei 25.326, de 4 de outubro de 2000), sendo ela considerada em

---

[65] "Conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.". (BRASIL, 1988).

[66] Como reflete Danilo Doneda (2006, p. 337): " Um sistema de proteção de dados pessoais que tenha como instrumentos principais de atuação o recurso a uma ação judicial (e com isso somente após um inafastável périplo administrativo) não se nos apresenta como um sistema adequado às exigências da matéria. Os problemas relacionados ao tratamento de dados pessoais, conforme observamos, processam-se cada vez mais "em branco", sem que o interessado se aperceba. Este, nas situações em que sabe ou suspeita que seus dados armazenados em algum banco de dados sejam errôneos, ou então tem conhecimento do seu uso indevido – ou mesmo deseja simplesmente fazer uma verificação – encontra-se diante da necessidade de recorrer a uma incerta via administrativa (cujo não atendimento, aliás, não acarreta penalidade objetiva ao responsável pelo armazenamento dos dados) e, no insucesso desta tentativa, deve utilizar-se do *habeas data* que, ao contrário do *habeas corpus*, exige um advogado para sua interposição – um tratamento bastante inadequado para um interesse cuja atuação pede o recurso a instrumentos promocionais."

.

"[...] sintonia com os preceitos básicos do modelo europeu de proteção de dados pessoais" (DONEDA, 2006, p. 350).

Em relação às regras dispostas no Código de Defesa do Consumidor, especificamente nos seus artigos 43 e 44[67], referente ao banco de dados e cadastro dos consumidores, em comparação com o *habeas data,* são muito mais avançadas e protetivas (LIMBERGER, 2007). No entanto, ainda sim possuem limites a sua incidência às relações de consumo (DONEDA, 2006, p. 340). Limberger (2007, p. 190) lembra que apesar destas limitações, há aspectos positivos, como a abrangência do Serviço de Proteção ao Crédito ou as listagens de mala-direta, que embora se tratem de atividade privada, tem-se um tratamento de caráter público das informações, nos termos do artigo 1º, § único, da Lei[68].

Deste modo, é possível identificar a influência de normas relativas à proteção de dados e alguns de seus princípios, como o da transparência, prevista no artigo 44, § 2º, resguardando um direito do consumidor de ser comunicado de que a informação a seu respeito está sendo processada. Outros direitos podem ser apontados, como o direito de acesso e de retificação (artigo 43, *caput).*

Embora, no direito brasileiro, o Código de Defesa do Consumidor tenha sido reconhecido por muito tempo a norma que mais diretamente abordava a proteção de dados, influenciando inclusive que muitas normas passassem a ser avaliadas através da sua óptica, a temática e sua complexidade e abrangência exigiu do ordenamento jurídico nacional um trato mais específico (DONEDA, 2015, p. 381). Assim, pode-se destacar a promulgação de leis que de forma direta, ainda que setorial, tratam a proteção de dados pessoais, trazendo consigo alguns

[67] "Art. 43. [...] § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. [...] § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. Art. 44. Os órgãos públicos de defesa do consumidor manterão cadastros atualizados de reclamações fundamentadas contra fornecedores de produtos e serviços, devendo divulgá-lo pública e anualmente. A divulgação indicará se a reclamação foi atendida ou não pelo fornecedor. § 1° É facultado o acesso às informações lá constantes para orientação e consulta por qualquer interessado. § 2° Aplicam-se a este artigo, no que couber, as mesmas regras enunciadas no artigo anterior e as do parágrafo único do art. 22 deste código.". (BRASIL, 1990).

[68] "Art. 1° O presente código estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, nos termos dos arts. 5°, inciso XXXII, 170, inciso V, da Constituição Federal e art. 48 de suas Disposições Transitórias.". (BRASIL, 1990).

de seus princípios, como a Lei de Cadastro Positivo[69] (Lei nº. 12.414/11), Lei de Acesso à Informação[70] (Lei nº. 12.527/11) e o Marco Civil da Internet (Lei nº. 12.965/14).

O Marco Civil da Internet[71] surgiu em oposição a um projeto de lei que tinha por objetivo a criação de uma legislação criminal para a internet no Brasil. Disciplina alguns aspectos da proteção de dados, mas não se trata de uma lei geral sobre o tema como as leis nacionais abordadas no subcapítulo anterior. Em verdade, o Marco Civil da Internet se apresenta como uma nova forma de regulação na sociedade da informação que procura estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil (LUCCA, 2015, p. 28).

Para Lemos (2015, p. 98 e 100), "Mesmo que não seja perfeito, o Marco Civil é hoje reconhecido no Brasil e no exterior como um modelo promissor para a relação entre o direito e a tecnologia.". Segundo Getschko (2015, p. 103), "[...] o Marco Civil inova na proteção à Internet e confirma o acerto das concepções brasileiras de como se posicionar em face à revolução que a Internet representa e da qual temos, ainda, uma pálida e incompleta visão.".

É importante ressaltar que antes da vigência da lei, segundo Magrani (2019, p. 73):

> [...] a ausência de disposições sobre direitos fundamentais básicos como a liberdade de expressão, o acesso ao conhecimento e o direito à privacidade dificultavam a aplicação da legislação em vigor e geravam inúmeras decisões jurídicas conflitantes para as mais diversas controvérsias envolvendo a internet.

Sobre as normas de proteção de dados no Marco Civil da Internet, vale anotar de início, a distinção prevista no artigo 3º, incisos II e III, que trata dos princípios do uso da internet no

---

[69] "Art. 5º São direitos do cadastrado: I - obter o cancelamento do cadastro quando solicitado; II - acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado; III - solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação; IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e VII - ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados." (BRASIL, 2011b).

[70] "Art. 4º Para os efeitos desta Lei, considera-se: [...] IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação [...]". (BRASIL, 2011b).

[71] Conforme aborda Lemos"[...] o marco civil da internet brasileira deverá ser ao mesmo tempo principiológico e normativo. Na parte principiológica, ele deverá definir os princípios basilares do desenvolvimento da rede no país. Na parte normativa, ele deverá cuidar das diversas lacunas presentes na lei brasileira, especialmente no que tange a estabelecer um regime geral de tutela da privacidade, da responsabilidade civil dos provedores e dos direitos e garantias fundamentais da rede.". (LEMOS, 2015, p. 98 e 100).

Brasil[72], entre a proteção da privacidade e a proteção dos dados pessoais, tal qual acontece na Carta de Direitos Fundamentais da União Europeia (artigo 7º e 8º) [73]. Segundo Doneda (2015, p. 382), "A inclusão em separado dos princípios de privacidade e proteção de dados evoca a sistemática segundo a qual a proteção de dados, ainda que ligada histórica e funcionalmente à tutela da privacidade, dela é distinta por possuir um escopo diverso.".

Além disto, estão presentes também vários princípios de proteção de dados. No seu artigo 7º, que trata do acesso à internet como essencial para o exercício da cidadania assegurando direitos aos usuários[74], prevê no inciso VIII os princípios fundamentais da proteção de dados, como o da transparência e o da finalidade. O consentimento (artigo 7º, inciso IX) e o princípio de segurança (artigos 13 e 15) também estão presentes no Marco Civil.

No entanto, a proteção de dados no Marco Civil da Internet é apenas definida como direito, não garantindo suficientemente uma adequada tutela dos dados pessoais no Brasil (ZANATTA, 2015, p. 463). Somente após a entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (Regulamento EU nº 2016/679), que no Brasil, após muitos anos sem ter uma lei geral sobre o tema, foi aprovada a Lei nº 13.709/18, que dispõe sobre a proteção de dados pessoais (entrando em vigor em agosto de 2020).

---

[72] "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.". (BRASIL, 2014).

[73] Ver notas 36 e 37.

[74] "Art. 7º. O acesso à Internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; [...] e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.". (BRASIL, 2014).

A aprovação da primeira lei geral de proteção de dados no país, tal como aconteceu nos demais países que anteriormente legislaram sobre a matéria, como visto na primeira geração nos países europeus, foi fruto de demanda e esforço de setores da sociedade civil na luta pela garantia de respeito aos direitos humanos e direitos fundamentais. A Organização Não-Governamental Coalizão Direitos na Rede, por exemplo, lançou uma campanha denominada "Seus Dados São Você: Liberdade, Proteção e Regulação", com o objetivo de alertar os cidadãos para os riscos do uso das informações pessoais e chamar sua atenção para a necessidade da aprovação de uma lei geral de proteção de dados pessoais.

> E aqui se inscreve a sanção presidencial, em 14 de agosto de 2018, da Lei Geral de Proteção de Dados Pessoais (LGPD). Naquela ocasião, participamos de uma ampla coalizão social de mais de 80 entidades, liderada pela Associação Brasileira das Empresas de Tecnologia da Informação e da Comunicação e por outras entidades, que defenderam, perante o Presidente da República, que a sanção da LGPD tratava-se de um grande pacto social de importância histórica e social similar àquela tida pela promulgação da Consolidação das Leis do Trabalho (CLT), pelo presidente Getúlio Vargas, em 1943. A CLT pacificou uma sociedade dividida e pavimentou o desenvolvimento industrial brasileiro no Século XX. A LGPD assume, guardadas as devidas proporções, função muito parecida no atual contexto brasileiro. (GUTIERREZ, 2019, p. 392)

Neste aspecto convém destacar que a Lei 13.709/2018 (LGDP) é composta por 10 (dez) capítulos: 1) disposições preliminares; 2) do tratamento de dados pessoais; 3) dos direitos do titular; 4) do tratamento de dados pessoais pelo poder público; 5) transferência internacional de dados; 6) dos agentes de tratamento de dados pessoais; 7) da segurança e das boas práticas da fiscalização; 9) da Autoridade Nacional de Proteção de Dados e do Conselho nacional de Proteção de dados pessoais; e, 10) disposições finais e transitórias.

Nela, podem ser apontadas duas características principais, a de se aproximar do Regulamento Geral de Proteção de Dados da União Europeia e apresentar elementos típicos do ordenamento jurídico brasileiro (DONEDA, MENDES, 2019). Em relação às semelhanças com o direito brasileiro, ressaltam-se os já apontados instrumentos jurídicos nacionais como o Marco Civil da Internet, em que prevê a proteção de dados como um fundamento do uso da Internet no Brasil, a Lei de Cadastro Positivo, que em seu artigo 5ª, VI, contempla a revisão de decisões automatizadas, e o Código de Defesa do Consumidor, mencionado pela Lei Geral de Proteção de Dados brasileiro no seu art. 64 como diálogo das fontes e na inversão do ônus da prova nos termos dos seus artigos 42 a 44 (DONEDA, MENDES, 2019).

Como aproximações com o sistema europeu de proteção de dados, pode-se apontar a exigência de uma base legal para o tratamento de dados, a adoção de princípios gerais e regras e a criação de uma autoridade independente de proteção de dados (DONEDA, MENDES,

2019). Doneda e Mendes (2019) apontam também como característica da primeira lei geral de proteção de dados aprovada no Brasil a convergência internacional em termos de princípios básicos de proteção de dados no mundo[75] e ainda ter como fundamento a diminuição do risco. Veja-se que os princípios basilares do Regulamento Geral de Proteção de Proteção de Dados Pessoais foram todos mantidos, "[...] enaltecendo o poder do cidadão sobre a gestão efetiva, clara e transparente de seus dados pessoais e buscando viabilizar um equilíbrio entre o público e o privado, o econômico e o social dentro desta sociedade informacional.". (RUARO, GLITZ, 2019, p. 352).

Conforme já visto, o Regulamento Geral de Proteção de Dados visou harmonizar as leis de privacidade em todos os Estados-Membros da União Europeia, assim como garantir maior proteção e direitos aos cidadãos europeus residentes no território. A lei brasileira, por sua vez, sofreu forte influência europeia e seu artigo 3º[76] prevê a proteção de dados do cidadão, independentemente de quem realize o tratamento, aplicando-se, portanto, aos Estados e ao mercado, abrangendo também o tratamento de dados realizado na Internet (artigo 1º) [77].

Portanto, a autodeterminação informativa, que é o principal pilar da regulação europeia, também o é da LGPD. Há também outras semelhanças entre o marco normativo europeu sobre proteção de dados e a trajetória brasileira sobre o tema. O conceito de dados pessoais e de dados sensíveis[78] adotados na Lei Geral de Proteção de Dados brasileira, disposto nos artigos 1º e 5º, inciso I, também se assemelha aos primeiros conceitos desenvolvidos como o da Convenção 108 do Conselho da Europa de 1981. Neste ponto, se destaca o papel da autoridade de proteção de dados para determinar a elaboração de relatório de impacto de privacidade em operações de tratamento de dados sensíveis, como tendência legislativa no marco regulatório de proteção de dados da União Europeia de, em que pese a tendência dominante da autodeterminação informativa, se preocupar com a regulação do risco e uma atuação *ex ante.*

---

[75] "[...] conceito esse que ficou conhecido a partir da tese de Colin Bennett.". (DONEDA, MENDES, 2019, p. 311).

[76] "Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.". (BRASIL, 2018).

[77] "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.". (BRASIL, 2018).

[78] "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável. II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural [...]". (BRASIL, 2018).

Do mesmo modo, ocorre em relação aos princípios de proteção de dados[79], como a transparência, exatidão, finalidade, livre acesso e segurança física e lógica, e formam "[...] a espinha dorsal de inúmeras normas existentes atualmente, como o GDPR [...], sendo importante ressaltar que os princípios deverão ser cumpridos, independente das bases legais para o tratamento dos dados pessoais." (VAINZOV, 2019, p. 138). Neste sentido, anotam Doneda e Mendes (2019, p. 314-315):

> O estabelecimento de uma série de princípios de proteção de dados e de direitos do titular dos dados pela Lei procura garantir, por um lado, um arcabouço de instrumentos que proporcionem ao cidadão meios para o efetivo controle do uso de seus dados por terceiros. Por outro, confere unidade sistêmica à própria disciplina da proteção de dados pessoais – que, seja pelas suas características intrínsecas seja pelo fato de se inserir em uma tradição já amadurecida em diversos outros países, se insere em nosso ordenamento com características próprias, que se deixam entrever talvez com maior relevância justamente ao se atentar para a particularidade dos princípios e direitos próprios à matéria.

Embora possuam nomenclaturas diferentes, os princípios são praticamente idênticos entre o sistema europeu e a lei brasileira. O princípio da finalidade exige que seja respeitada sua correlação com o informado para o tratamento dos dados, o da necessidade visa restringir os dados coletados ao estritamente necessário para o cumprimento da finalidade informada. Ademais, muitos princípios já estavam presentes em outras leis brasileiras que não tratavam exclusivamente de proteção de dados pessoais[80].

A LGPD adota, portanto, um sistema de normas que envolvem princípios e direitos que limitam o tratamento de dados pessoais ao mesmo tempo em que empoderam o cidadão para controlar o fluxo dos seus dados. Novos direitos contemplados pelo Regulamento Geral de

---

[79] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.". (BRASIL, 2018).

[80] Ver notas 67, 69, 70, 72 e 73.

Proteção de Dados, como a portabilidade dos dados, também estão previstos na lei brasileira (artigo 18, inciso V, da LGPD).

E também, assim como faz o Regulamento Geral de Proteção de Dados, a LGPD também se ampara no princípio da *accountability*. Doneda e Mendes (2019, p. 375) lembram que "A lei procura ainda abordar aspectos contemporâneos da proteção de dados, como o desenvolvimento de medidas relacionadas à privacidade na concepção", disposta no artigo 46, § 2º[81].

Ressaltam-se as semelhanças no que toca à obrigação dos agentes controladores[82] e a segurança da informação[83], como por exemplo, o dever de realizar relatórios de impacto à privacidade[84]. No que tange às sanções pelo descumprimento da lei, há muitas semelhanças. Mas sua aplicação depende da constituição de uma autoridade de proteção de dados independente, o que destaca a importância de sua constituição e bom funcionamento.

> Uma análise das mais de 40 hipóteses do texto legal em que a autoridade é chamada para atuar demonstra que a sua competência vai desde a solicitação e análise de relatório de impacto de privacidade, determinação de medidas para reverter efeitos de vazamentos de dados, disposição sobre padrões técnicos de segurança da informação até a autorização da transferência internacional de dados pessoais. Isso demonstra que o órgão não é um mero coadjuvante do sistema de proteção de dados: ao contrário, é seu pilar de sustentação, sem o qual todo o arcabouço normativo e principiológico não está apto a funcionar de forma adequada. (DONEDA, MENDES, 2019, p. 319).

Sabe-se que o estabelecimento de uma autoridade independente é fundamental para a regulação do tema, como dispõe o regulamento europeu, considerando que a mesma deve monitor o Estado e o mercado. Seu papel é fiscalizar e aplicar da lei de proteção de dados,

---

[81] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.". (BRASIL, 2018).

[82] Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

[83] Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

[84] Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

aumentando a possibilidade de uma maior proteção da privacidade e dos dados pessoais das pessoas naturais.

Contudo, a autoridade nacional de proteção de dados foi vetada, em um primeiro momento, na LGDP[85]. Tal fato fez com que várias entidades brasileiras protestassem contra o veto. O Instituto de Tecnologia e Sociedade do Rio de Janeiro, por exemplo, elaborou um relatório com uma proposta para a criação da autoridade brasileira de proteção de dados pessoais (2018), demonstrando a experiência de outros países que constituíram autoridades nacionais de proteção para aplicar de maneira eficiente suas respectivas leis de proteção de dados pessoais, como Reino Unido, França, Itália, Argentina e Uruguai.

> Não há dúvida de que uma maior compatibilidade entre os diferentes sistemas facilitará, por exemplo, os fluxos informacionais de dados, o que beneficiará os mais diversos setores e poderá ser utilizado para variados fins, como comerciais e para a cooperação entre entidades públicas (ITS RIO, 2018, p. 04).

Na América Latina, boa parte dos países adotou ou passou a considerar a adoção de legislação a este respeito (DONEDA, MENDES, 2019). Entretanto, apenas Argentina e Uruguai são considerados países que são reconhecidos como modelos adequados de tratamento de dados pessoais estabelecido na Europa, tendo suas análises verificada especialmente pela independência através de fatores como estrutura e organização, exercício das funções e atribuições e poderes da autoridade (ITS RIO, 2018, p. 04).

Como salientado pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro (2018), para que o Brasil alcance um patamar elevado de proteção aos direitos humanos e de desenvolvimento enquanto nação, era preciso criar uma Autoridade Nacional de Proteção de Dados pessoais que seja autônoma, independente, com características semelhantes àquelas preconizadas na norma europeia de proteção de dados. Além disso, vários pontos dependem de regulamentação pela Autoridade Nacional, o que prejudicaria setores produtivos e inviabilizam uma flexibilização de normas independentes do tamanho ou atividade da empresa (ITS RIO, 2018, p. 06).

---

[85] O veto alegou que a primeira empresa que sofresse uma sanção poderia alegar a inconstitucionalidade da autoridade, o que geraria uma insegurança jurídica e uma complexa demanda ao judiciário. "No Brasil, os principais argumentos que embasaram o veto à autoridade na Lei n. 13.702018 envolveram, essencialmente, a possibilidade de vício de iniciativa e questões orçamentárias. Alegou-se que uma iniciativa do legislativo não poderia criar um órgão como a mencionada autoridade. Isso só poderia ser feito pelo Executivo, com base nos artigos 61, § 1º, II e 37, XIX, da Constituição Federal de 1988. Afirmou-se também que o projeto não poderia criar estes não previstos no orçamento, uma vez que a autoridade geraria despesas para a sua implementação e funcionamento. Além disso, vale lembrar que a lei foi aprovada pelo Senado em 10 de julho de 2018, data próxima ao período eleitoral, o que possivelmente criou e vem gerando um desafio ainda maior para a criação da entidade" (ITS RIO, 2018, p. 11).

A Autoridade Nacional da Proteção de Dados (ANPD) foi então aprovada pela Lei 13.853/19, em 08 de julho de 2019[86], disposta no capítulo XIX da LGPD, dentre os artigos 55-A ao 58-A. Embora em nenhum momento se afirme categoricamente que a autoridade nacional deva ser independente no seu texto, ao contrário das normas de proteção de dados da União Europeia[87], da há garantia de sua estabilidade e a autonomia técnica e financeira, previstas no artigo 55-B e 55-E da LGPD. Lucca e Lima (2019, p. 375), ressaltam que para "[...] a efetividade do sistema de proteção de dados, essa entidade deve ter absoluta independência funcional e autonomia financeira para que possa tomar decisões imparciais. Nesse sentido, o art. 55-B da LGPD assegura a autonomia técnica e decisória da ANPD[88].".

O artigo 55-E prevê que os membros do Conselho Diretor somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo administrativo disciplinar, tal como consta nas regras do Regulamento Geral de Proteção de Dados (artigo 53, item 3)[89].

A forma de escolha dos diretores da Autoridade Nacional de Proteção de Dados[90], exigindo aprovação do Senado Federal após indicação do presidente do poder executivo, contribui também para a sua independência (LUCCA E LIMA, 2019, p. 375). Quanto a duração do cargo, deve-se observar para que não coincida com os mandatos do chefe do poder executivo, aumentando assim sua autonomia política.

Em relação à sua estrutura, ainda que tenha sido criada como órgão da administração pública direta, vinculada à Presidência da República de forma inicial e transitória, eis que após

---

[86] Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.". (BRASIL, 2018).

[87] Ver notas 27, 28 e 29.

[88] Há discordância na doutrina quanto a garantia de independência e autonomia da autoridade nacional na LGPD apenas pelo disposto no seu artigo 55-B, como é o caso de Vasconcelos e Paula (2019, p. 731).

[89] Ver nota 53.

[90] "Art. 55-D. O Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo em comissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. § 2º Os membros do Conselho Diretor serão escolhidos dentre brasileiros que tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos para os quais serão nomeados. § 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. § 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. § 5º Na hipótese de vacância do cargo no curso do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor. (BRASIL, 2018).

02 (dois) anos será reapreciada a possibilidade de transformá-la em uma agência reguladora (LUCCA E LIMA, 2019, p. 392). O Instituto de Defesa do Consumidor - IDEC (2019), em pesquisa realizada com o objetivo de identificar e avaliar modelos de autoridades de proteção de dados pessoais na América Latina, afirmou que a brasileira, ao estar administrativamente vinculada à Presidência da República, tem comprometida sua independência (2019, p. 17).

O Regulamento Geral de Proteção de Dados prevê, por exemplo, que as autoridades de proteção de dados deve ter asseguradas condições eficazes para as suas atribuições e exercício de seus poderes[91]. Como ressalta a Agência de Direitos Fundamentais de União Europeia (2010, p. 38), o melhor modelo é "[...] aquele cuja a autoridade possua personalidade jurídica própria, estando desvinculada da administração direta, e a nomeação de seus membros passem pelo crivo da oposição, como no Congresso ou admita a participação da sociedade civil nesta escolha.".

Em relação à independência financeira, o artigo 55-L da LGPD contempla que constituem suas receitas, as dotações, consignadas no orçamento geral da União, os créditos especiais, os créditos adicionais, as transferências e os repasses que lhe forem conferidos, as doações, os legados, as subvenções e outros recursos que lhe forem destinados, valores apurados na venda ou aluguel de bens móveis e imóveis de sua propriedade, e, os valores apurados em aplicações no mercado financeiro das receitas previstas neste artigo.

Neste ponto, na medida em que o Regulamento Geral de Proteção de Dados da União Europeia estabelece que os Estados-membros devem assegurar estes recursos[92], e que também as receitas da Autoridade Nacional de Proteção de Dados brasileira não difere da forma adotada na maioria dos países europeus e do mundo, como visto no subcapítulo anterior, sua independência financeira pode ser considerada, no plano normativo, assegurada.

Porém, como defendem Lucca e Lima (2019, p. 393-394), em razão da velocidade dos avanços tecnológicos, a autoridade nacional necessita de uma equipe multidisciplinar para desempenhar suas funções, sendo que as receitas previstas na LGPD não parecem suficientes, e uma fonte possível, advinda da fiscalização das empresas, foi vetada na lei. Esta preocupação é reforçada, eis que estudos demonstram ser esta uma dificuldade em alguns países da União Europeia (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 22) e na América Latina (INSTITUTO DE DEFESA DO CONSUMIDOR, 2019, p. 35).

[91] Ver nota 53.
[92] Idem.

A competência da Autoridade Nacional de Proteção de dados brasileira está disposta no artigo 55-J[93]. Sua ênfase encontra-se nas funções preventivas e fiscalizatórias, engendrando todos os esforços necessários para a prevenção de danos aos dados pessoais, como vazamentos e tratamentos ilegais, e fiscalização para o efetivo cumprimento da lei, pois "[...] quando ocorre uma violação aos princípios e direitos estabelecidos na LGPD, dificilmente é possível retornar ao *status quo."*. (LUCCA, LIMA, 2019, p. 385). Ademais,

> [...] nessa área tão dinâmica, uma vez que a coleta e o tratamento dos dados pessoais são realizados em massa por sistemas de informação e circulam na internet, dado o crescente uso da web em diversas áreas, essa competência da ANPD será fundamental para manter a LGPD sempre adaptada às novas tecnologias e modelos de negócios sem ter de alterar a lei, dada a demora do processo legislativo. (LUCCA, LIMA, 2019, p. 386).

[93] "Art. 55-J. Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação; VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; XII - elaborar relatórios de gestão anuais acerca de suas atividades; XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas; XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei; XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso); XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.". (BRASIL, 2018).

Ainda, “A futura ANPD também deverá se debruçar sobre o conteúdo dos relatórios de impacto à proteção de dados pessoais, assim como nos casos em que o mesmo será obrigatório.”. (GUTIERREZ, 2019, p. 395). É o caso, por exemplo, do tratamento de dados sensíveis, em que a LGPD, no seu artigo 11, § 3º, prevê que a comunicação ou o seu uso compartilhado entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional.

E neste sentido, também cabe enfatizar o papel e futura atuação do Conselho nacional de Proteção de Dados[94], previsto na LGPD. Como visto, no sistema europeu de proteção de dados, o Conselho Europeu de Proteção de Dados funciona como autoridade responsável por decidir casos de conflitos de autoridades nacionais de proteção em aplicação transfronteiriça[95], e a Autoridade Europeia de Proteção de Dados possui funções semelhantes ao conselho brasileiro.

Na lei brasileira, suas funções se complementam com as da autoridade de proteção de dados. Sua composição será de 23 (vinte e três) representantes, entre titulares e suplentes, de vários órgãos, como do Poder Executivo federal, Congresso Nacional, Conselhos Nacionais da Justiça e do Ministério Público, Comitê Gestor da Internet no Brasil, sociedade civil, academia, confederações sindicais, setor empresarial e laboral (artigo 58-A da LGPD). A composição multisetorial, portanto, do Conselho Nacional de Proteção de Dados brasileiro se assemelha ao do Comitê Gestor da Internet, que tem a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e políticas de governança que define o nome de domínio brasileiro, e, se constitui em “[...] uma conquista inovadora em gestão pluralista de bens da comunidade.”. (KURBALIJA, 2016, p. 237). É como pensam Lucca e Lima (2019, p. 383-383):

> A composição do Conselho Nacional de Proteção de Dados e Privacidade é interessante, pois propicia um natural sistema de freios e contrapesos *interna corporis*, colaborando para a autonomia técnica da ANPD, pois os representantes do setor privado serão constantemente fiscalizados pelos representantes do setor público e vice-versa. Portanto, seus integrantes devem ser especialistas na área e com notável atuação na área de proteção de dados pessoais, para que tenham um absoluto comprometimento com as atribuições da autoridade brasileira, atraindo, então, o reconhecimento pela União Europeia.

[94] “Art. 58-B. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD; II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade; III - sugerir ações a serem realizadas pela ANPD; IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.”. (BRASIL, 2018).

[95] Vide notas 57 e 58.

Nas primeiras discussões, no ano de 2010, sobre a adoção de uma lei geral de proteção de dados no Brasil aos moldes de um sistema europeu, quanto a adoção de uma autoridade de controle independente, se chegou a discutir que o melhor modelo a ser adotado seria o do Comitê Gestor da Internet, "[...] conhecido pelo formato "multisetorial" de deliberação, no qual empresas privadas, comunidade acadêmica, membros do governo e representantes da sociedade civil têm espaço para discussão horizontal.". (ZANATTA, 2015, p. 461). No entanto, o modelo adotado na LGPD não foge à regra dos processos de nomeação das demais autoridades nacionais do mundo, onde diversos métodos, a depender das disposições constitucionais que regem o estabelecimento de autoridades independentes, como eleição, escolha pelo executivo, legislativo, sociedade civil e outros (INTERNACIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS, 2017).

Diante da opção brasileira pela corregulação, a "[...] ANPD desempenhará suas funções fiscalizadora, reguladora e sancionatórias, sem excluir a possibilidade de os agentes de tratamento de dados pessoais estabelecerem "Boas Práticas" (art. 50 da LGPD).". (LUCCA, LIMA, 2019, p. 376). A criação de uma autoridade nacional é indispensável para a proteção de dados, e mais ainda "[...] é passo imprescindível para a efetiva aplicação da Lei Geral de Proteção de Dados no Brasil". (VASCONCELOS, PAULA, 2019, p. 374).

> [...] está claro que o Brasil precisava de uma Lei Geral de proteção de Dados Pessoais, bem como de um órgão independente para o controle e fiscalização do cumprimento da lei, tal como ocorre em vários países do mundo. Só assim poderão as empresas brasileiras receber dados de cidadãos europeus e de cidadãos de outros continentes, preservando-se a necessária reciprocidade entre os países. Tomando por base o capitalismo informacional, tal exigência é crucial para que as empresas brasileiras possam competir em igualdade de condições com as empresas de outros países. (LUCCA E LIMA, 2019, p. 380).

No aspecto normativo, há muitas semelhanças na constituição das autoridades de proteção europeias e a brasileira. Entretanto, em relação aos poderes, houve críticas em relação ao seu reduzido rol em comparação com o Regulamento Geral de Proteção de Dados, como por exemplo, ao não contemplar a possibilidade de realizar busca e apreensão e obter acesso a todas as instalações, equipamentos e meios de tratamentos de dados, acesso aos dados e todas informações necessárias ao exercício de suas funções de responsável pelo tratamento[96]. Mesmo as autoridades da América Latina possuem amplos poderes de investigação conferidos pela legislação (INSTITUTO DE DEFESA DO CONSUMIDOR, 2019, p. 37).

[96] Vide nota 55.

Existem atualmente no mundo cerca de 83 (oitenta e três) países que adotaram autoridades de proteção de dados, sendo aqueles que ainda não o fizeram após a vigência de uma lei geral de proteção de dados considerado participantes da "Calçada da vergonha", nos termos utilizados por Greenleaf (2017). Diante disso pode-se dizer que o Brasil está atualmente em uma travessia, pois ainda não está em vigência sua lei.

No entanto, considerando ser essencial a atuação da Autoridade Nacional de Proteção de Dados para a efetivação deste direito fundamental, sua constituição deve ocorrer o mais breve possível.

> Se há pouco mais de um ano e meio para as organizações brasileiras se adequarem à nova legislação, a ANPD deveria começar o quanto antes o trabalho de regulamentação da LGPD e de detalhamento dos pontos obscuros ou dúbios. Sem essas balizas e orientações, o trabalho de conformidade pelas organizações ficará muito prejudicado. O tempo aqui também pode ser amigo ou inimigo da conformidade legal. (GUTIERREZ, 2019, p. 395).

A Argentina, reconhecida pela União Europeia como um país com bom nível de proteção, o que possibilita a transferência internacional dos dados (LUCCA, LIMA, 2019. p. 378), teve sua autoridade nacional criada em 2001. Em 2017, para se adequar ao Regulamento Geral de Proteção de Dados da União Europeia, aprovou a Agência de Acesso à Informação Pública, na forma de autarquia, sendo classificada como independente, autônoma funcional e financeiramente, com previsão de mandato fixo e pessoal técnico e administrativo dedicado.

Deste modo, é preciso continuar o desenvolvimento de uma cultura de proteção de dados no Brasil, tendo a autoridade independente papel decisivo para incentivar e coordenar ações que visem informar o cidadão sobre seus direitos frente o processamento de dados, bem como gerar confiança jurídica para o desenvolvimento de uma economia de dados com fluxo apropriado. Por isso, o Brasil deve, para se adequar a um adequado tratamento jurídico do tema, adotar um sistema de autoridade de proteção independente, na forma de autarquia, tal qual funciona outros órgãos da administração pública.

Apesar de poderes reduzidos no aspecto normativo em relação aos padrões do sistema europeu e suas possíveis consequências para a proteção de dados pessoais, em princípio isto não impediria o reconhecimento da União Europeia, eis que foi possível observar em estudos citados anteriormente sobre autoridades de proteção que nem todas possuem o mesmo rol de ações (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010). Veja-se que na decisão da Comissão Europeia, ao entender ser o nível de proteção de dados do Uruguai adequado ao estabelecido na União Europeia, considerou, dentre outros aspectos, que ainda que

não contemple de modo explícito o direito à proteção de dados em sua constituição, seu reconhecimento de um nível de proteção adequado pela União Europeia se deu pela existência de uma lei geral de proteção e uma autoridade nacional de controle:

> [...] (5) A Constituição da República Oriental do Uruguai, aprovada em 1967, não reconhece expressamente o direito ao respeito pela vida privada e à proteção dos dados pessoais. Contudo, a enumeração dos direitos fundamentais não constitui uma lista fechada, dado que o artigo 72.o da Constituição determina que a lista de direitos, obrigações e garantias previstos na Constituição não exclui outros que sejam inerentes à personalidade humana ou que derivem da forma republicana de governo. O artigo 1.o da Lei n.o 18.331 de proteção de dados pessoais e ação de habeas data, de 11 de agosto de 2008 (Ley n.o 18.331 de protección de datos personales y acción de habeas data) prevê expressamente que «o direito à proteção dos dados pessoais é inerente ao ser humano, pelo que se encontra abrangido pelo artigo 72.o da Constituição da República». [...] (10) A aplicação das normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de habeas data, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento dos dados, a fim de exercer o direito de acesso, retificação e supressão, e por um controlo independente efetuado pela Unidade Reguladora e de Controlo de Dados Pessoais (Unidad Reguladora y de Control de Datos Personales – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28.o da Diretiva 95/46/CE, e que atua de forma totalmente independente. (2012).

Neste ponto, considerando que o Brasil possui uma lei geral de proteção de dados que contempla uma autoridade de proteção de modo semelhante ao sistema europeu de proteção de dados, e ainda um quadro jurídico bastante parecido ao do Uruguai, é possível afirmar que o mesmo pode também ter o igual reconhecimento. Obter essa aprovação é positivo para a segurança jurídica no comércio e cooperação internacional (2019, INSTITUTO DE DEFESA DO CONSUMIDOR, p. 08).

Conforme afirma o Instituto de Defesa do Consumidor - IDEC (2019, p. 08), os países da América Latina estão atualmente em um estado de transição, e "A garantia constitucional passa a ser combinada ao surgimento de leis gerais que regulamentam qualquer tratamento de informações pessoais, sejam elas privadas ou não, e a proteção a esse direito é feita também na seara administrativa por meio de autoridades de proteção.". Mas, considerando o atraso regulatório do Brasil em relação a outros países da América Latina, que nos últimos anos passaram a legislar sobre a proteção de dados pessoais com a definição de direitos dos cidadãos e a criação de mecanismos de cumprimento de tais direitos via agências reguladoras, seria recomendável uma previsão constitucional do direito à proteção de dados pessoais, como ocorreu na maioria dos países e também recomendado na União Europeia (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 22). Ainda, é preciso reconhecer a autoridade de proteção como exigência deste direito já na norma constitucional.

No Senado Federal brasileiro, encontra-se uma proposta de Emenda à Constituição nº 17/2019, visando modificar o inciso XII-A do artigo 5º[97] e o inciso XXX ao artigo 22[98] da Constituição Federal. Em suma, pretende-se incluir a proteção de dados como um direito fundamental e fixar a competência privada da União para legislar sobre a matéria. Como justificativa, o projeto aborda a proteção de dados e sua evolução histórica na sociedade informacional, os riscos que representa às liberdades e garantias individuais do cidadão, o impacto global do Regulamento Geral de Proteção de Dados da União Europeia e discussão do assunto como um direito autônomo e constitucional.

Entretanto, em comparação com o disposto na Carta de Direitos Fundamentais da União Europeia, não está disposto a garantia de uma autoridade independente para o cumprimento da lei[99], o que poderia ser acrescido ao texto legal, eis que ainda não votado. Como defende Mendes (2018, p. 06):

> Sem a construção dessa arquitetura regulatória, não será possível alcançar o seu principal objetivo, que é o de consolidar a confiança da sociedade na infraestrutura de informação e comunicação, garantindo direitos, ampliando a inovação e propiciando mais competitividade entre os serviços que utilizam dados pessoais de forma legítima e transparente. Nas últimas décadas, ficou claro que a existência de órgãos administrativos de proteção de dados pessoais é essencial para a implementação da legislação e da cultura da privacidade no Brasil.

Embora necessite de evidentes avanços no aspecto normativo, é preciso ressaltar que o sistema de proteção de dados brasileiro vem se desenvolvendo ainda que não possuísse uma lei geral. O Comitê Gestor da Internet, por exemplo, organiza um Seminário Anual sobre Proteção à Privacidade e aos dados pessoais, com a participação de acadêmicos internacionais e profissionais de diferentes áreas de atuação. Para Zanatta (2015, p. 455), "Desde 2010, tal seminário tem servido como ponto modal para a discussão da proteção de dados pessoais no Brasil e avaliação das políticas regulatórias propostas pelo governo.".

Em agosto de 2018, o Instituto de Defesa do Consumidor (IDEC) ajuizou ação civil pública com pedido de tutela de urgência contra a concessionária da linha 400 Metrô de São Paulo, conhecida como "Viaquatro", com o fim de cessar a coleta de dados de forma obrigatória dos consumidores por meio das "Portas Interativas Digitais". Conforme narrado nos fatos da

---

[97] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.". (BRASIL, 2019).
[98] Rol de competências privativas de legislar da União.
[99] Ver nota 37.

petição inicial (INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, 2018), a tecnologia implementada nessas portas, segundo a empresa, consiste em uma lente com um sensor que "reconhece a presença humana e identifica a quantidade de pessoas que passam e olham para tela", identificando emoções como raiva, alegria e neutralidade, além de gênero e faixa etária. O sensor é posicionado acima de uma propaganda publicitária, não havendo informações claras e detalhadamente sobre seu funcionamento. Como observa o IDEC (2018, p. 09):

> [...] a empresa nem mesmo oferece aos passageiros opção de decidir que não querem ter seus dados extraídos e processados nesse sistema, cujo funcionamento e finalidade são obscuros e dão margem a pesquisas de mercado sem consentimento dos consumidores, violando, assim, uma série de normas do ordenamento jurídico.

O Instituto de Referência em Internet e Sociedade –IRIS (2019) apresentou parecer técnico sobre o caso a pedido do IDEC. Foi constatado no parecer que a situação analisada consiste na violação à Constituição Federal, aos direitos dos consumidores e usuários de transporte público, bem como aos direitos de proteção de dados pessoais, aos direitos coletivos relacionados ao consentimento, à informação e autodeterminação dos usuários de metrô.

Estas ações são estratégicas para moldar um comportamento das empresas para que respeitem as regras sobre o tratamento de dados. Reforça-se, assim, o ecossistema de proteção de dados, com a participação de especialistas da sociedade civil em demandas que envolvam possíveis violações à legislação sobre o tema. A lei geral foi fundamental, mas é preciso pensar em regulação também através dos órgãos administrativos do Estado.

Por outro lado, evidencia-se a necessidade da imediata constituição de uma Autoridade Nacional de Proteção de Dados em razão das diversas violações de direitos humanos e fundamentais que podem ocasionar o tratamento de dados e estão ocorrendo no Brasil atualmente. Mas, se para os países desenvolvidos e mais adaptados aos desafios da sociedade da informação esta garantia institucional foi constatada e aperfeiçoada ao longo dos quase 50 anos de leis de proteção de dados, no Brasil é possível haver uma diminuição do problema se comparado a outras demandas sociais, como saúde e educação.

O grande desafio brasileiro após a aprovação de sua primeira lei geral de proteção de dados, com todas as características observadas nos demais países e necessárias para o tratamento de dados pessoais, é a instrumentalização e garantia da constituição de uma autoridade independente de proteção e que sua atuação seja garantida através de autonomia técnica e financeira. Assim, o Brasil teria um tratamento jurídico adequado do tema.

4. CONCLUSÃO

O tratamento de dados pessoais cada vez mais opera com técnicas sofisticadas ampliando assim a necessidade de proteção dos dados diante dos riscos aos direitos humanos e direitos fundamentais apontados pela literatura crítica das novas tecnologias, como o direito à privacidade, à liberdade, à igualdade e à democracia. A efetivação das leis de proteção de dados depende da atuação de uma autoridade de controle independente que seja capaz de fiscalizar o cumprimento da lei pelos Estados e pelo mercado e assim tutele os direitos do cidadão.

Ao final desta dissertação, retoma-se o problema de pesquisa: considerando os elementos e características da sociedade em rede, marcadas pelo intenso uso das tecnologias da informação e comunicação (TIC) e pelos novos riscos derivados dos fluxos informacionais, é possível afirmar, em perspectiva comparada, que o recente marco regulatório editado no Brasil referente à proteção de dados pessoais e criação da Autoridade Nacional de Proteção de Dados (ANPD) permitirá que o país seja considerado com o mesmo nível de proteção normativa da União Europeia?

Diante da análise bibliográfica e documental utilizada, é possível afirmar, levando-se em consideração o problema de pesquisa apontado, que com a aprovação de uma legislação nacional sobre o assunto, e com a constituição de uma Autoridade Nacional de Proteção de Dados, o Brasil pode postular legitimamente o reconhecimento do mesmo nível de proteção da União Europeia.

O modelo de proteção de dados europeu é o mais influente globalmente, visando a garantia de direitos e sua livre circulação objetivando um tratamento lícito e leal, desde as primeiras iniciativas legais no plano internacional como a Convenção 108 do Conselho Europeu de 1981, e para seu funcionamento é indispensável a existência de uma autoridade independente de controle. Do ponto de vista normativo, o Brasil possui as mesmas condições que levaram a Argentina e Uruguai ao reconhecimento de mesmo padrão de proteção da União Europeia, permitindo assim a transferência internacional dos dados e facilitando a inserção do país em uma economia de capitalismo informacional.

Contudo, para a efetiva proteção, é necessária uma autoridade independente. A previsão da autoridade de controle brasileira como integrante do poder executivo, já a compromete formalmente. Sem a autonomia técnica e financeira, não se pode garantir a fiscalização do tratamento de dados por parte do Estado e do mercado. Um fator que pode contribuir para que o Brasil atinja um tratamento jurídico adequado do tema é inserir o direito à proteção de dados como um direito fundamental na Constituição Federal.

Embora exista um projeto de emenda à constituição que define o direito à proteção de dados como direito fundamental no Brasil, fixando competência exclusiva da União Federal para legislar sobre o tema, nos moldes de leis gerais e de um padrão europeu de proteção, não há a menção de que este novo direito é garantido pela existência de uma autoridade responsável pela fiscalização deste, tal como ocorre no artigo 8º da Carta de Direitos Fundamentais da União Europeia e outros tratados. Com a criação de uma Autoridade Nacional de Proteção de Dados, o país segue o sistema europeu, que visa uma harmonização dos tratamentos jurídicos a respeito do tema como forma de mitigar os riscos aos direitos humanos e direitos fundamentais diante do fluxo informacional transnacional.

Diante destas constatações, pode-se dizer que se atingiu o objetivo geral da pesquisa. Ao se discorrer criticamente os riscos aos direitos humanos e direitos fundamentais derivados da utilização dos dados pessoais pelos Estados e pelo mercado, de modo a considerar algumas repercussões jurídicas, políticas e sociais do tratamento de dados, analisaram-se a necessidade de reconhecimento deste novo direito que exige novas formas de tutela e a sua importância nos dias atuais.

A ambivalência das novas tecnologias promove várias repercussões em direitos fundamentais, ampliando alguns direitos, como o direito à informação, e reduzindo outros, como o direito à privacidade. Exigiu o reconhecimento de novos direitos e novas formas de proteção em que as repercussões sociais e políticas devem permear debates sobre a regulação do tema.

Do ponto de vista do Estado, há uma tendência natural ao controle social, e o estabelecimento de limites ao tratamento de dados pessoais é uma função que cabe ao parlamento, o poder judiciário e a sociedade civil, mas principalmente a Autoridade Nacional de Proteção de Dados, devido à sua especialidade técnica. A existência de uma economia global forjada nas novas tecnologias amplia esta necessidade de tutela institucional ao tratamento de dados pessoais, cabendo uma forte atuação da autoridade para limitar este tratamento exigindo o cumprimento da lei e elaborando pareceres em projetos de lei sobre tais operações.

De outro lado, a atuação da autoridade nacional fortalece uma segurança institucional para o desenvolvimento de uma economia digital baseada na inovação e que precisa de regras seguras e confiáveis para desenvolver seus negócios. O modelo europeu de proteção tem essa dupla finalidade, a de garantir a livre circulação dos dados privilegiando um tratamento lícito e leal atento aos princípios de proteção de dados. Embora ainda não constituída ao tempo da presente pesquisa, o que prejudicou sua análise em termos de atuação, evidencia-se esta necessidade devido ao próprio favorecimento que proporcionará às empresas brasileiras.

Desse modo, resta clara a complexidade que envolve o tema da proteção de dados, onde, por exemplo, tem de ser balanceados direitos como a privacidade e o direito ao desenvolvimento, no sentido econômico do país. Ao se verificar e discutir o tratamento jurídico do tema em perspectiva comparada entre União Europeia e Brasil, examinando como estas legislações tratam da regulação dos fluxos informacionais e dos instrumentos delineados para a tutela dos dados, com ênfase para a atuação da Autoridade Nacional de Proteção de Dados, constatou-se a similitude dos sistemas de proteção de dados no plano normativo.

Em razão das críticas ao paradigma da autodeterminação informativa e a garantia de direitos através do livre consentimento, o modelo europeu de proteção de dados passou a se preocupar com os riscos do tratamento, em uma regulação que procura evitar os danos antes que eles ocorram. Para o funcionamento deste modelo de regulação delineado é indispensável a atuação da autoridade de controle para uma série de outras funções que vão além da fiscalização da norma. Produzir normas setoriais e dialogar com os diferentes setores, autorizar previamente e conceder licenças em tratamento de dados que impliquem em risco aos direitos dos cidadãos, promover campanhas educativas. Tais atribuições e poderes, em atuação, podem promover o adequado de tratamento jurídico do tema.

Obviamente, muitas violações sobre a proteção de dados ocorrem no país, como vazamento de dados e falta de segurança, tratamento de dados em desacordo com autorização legal e seus princípios, projetos governamentais de integração de bancos de dados sem a transparência de sua finalidade, dentre outros. Tais fatos somente reforçam que uma tutela individual para este novo direito é muito limitada, como nos casos de ações individuais de responsabilidade civil, em que pouco contribui para um fortalecimento de um tratamento de dados leal e lícito.

Não há razão para a insistência no direito brasileiro em crer da proteção de dados como mera decorrência e extensão do direito individual de privacidade, intimidade e vida privada, enquanto a maioria dos países já a reconhece como novo direito. Não se nega a importância destes direitos, mas outros direitos também fundamentais estão relacionados quando se trata do tema da proteção de dados.

As alegações de geração de aumento de despesas não são legítimas para impedir a constituição e atuação da Autoridade nacional de Proteção de Dados. Primeiramente, porque trata de uma garantia institucional que decorre do tratamento de dados por parte do Estado e seu dever de garantir os direitos dos titulares dos dados. Em segundo, porque trata de uma área sensível a constantes alterações que impedem uma legislação ágil e eficiente que somente é possível através de um conhecimento técnico específico.

No que se refere ao tratamento de dados pessoais pelo mercado, a existência de uma autoridade de controle é indispensável para a regulação do ambiente de competitividade das novas tecnologias, sem o qual impossibilita que o país ingresse em uma economia digital global. Portanto, as despesas e custos da criação de uma autoridade de controle são exigidos pelo capitalismo informacional. Além disso, as despesas necessárias para a sua autonomia técnica e financeira podem ser obtidas através de sanções a serem aplicadas em casos de violação à lei de proteção de dados, o que sem sua existência podem sequer serem conhecidas, o que lamentavelmente não foi aprovado na legislação brasileira.

Os riscos sociais e políticos do tratamento de dados pessoais apontados pela literatura crítica das novas tecnologias revelam o lado *orwelliano* do Estado em vigiar completamente o cidadão, e o lado "Admirável Mundo Novo" do mercado com a classificação das pessoas em categorias de consumidores. Os fatos recentes no campo da segurança interna e internacional e no que se refere ao funcionamento dos mercados, da globalização, das mídias e da relação entre cidadania, Estado e novas tecnologias reforçam esta preocupação e a necessidade de atuação desta autoridade.

REFERÊNCIAS

AGAMBEN, Giorgio. **Estado de exceção.** Tradução Iraci Poleti. São Paulo: Boitempo, 2004.

AGAMBEN, Giorgio. From the State of Control to a Praxis of Destituent Power. **The Anarchist Library**, p.1-7, 2013. Disponível em: http://theanarchistlibrary.org/library/giorgio-agamben-from-the-state-of-control-to-a-praxis-of-destituent-power.a4.pdf. Acesso em: 15 fev. 2020.

AGAMBEN, Giorgio. **Homo Sacer:** O poder soberano e a vida nua I. Trad. Henrique Burigo. Belo Horizonte: Editora UFMG, 2002.

AMNESTY INTERNATIONAL. **Israel:** Amnesty International engages in legal action to stop NSO Group's web of surveillance. 2019. Disponível em: https://www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance. Acesso em: 13 maio 2019.

ARAGÃO, Alexandre Santos de. O poder normativo das agências reguladoras independentes e o Estado democrático de Direito. **Revista de Informação Legislativa**, Brasília, p.1-25, 2000. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/646/r148-19.pdf. Acesso em: 15 fev. 2020.

ASSENGE, Julian et al. **Cypherpunks:** liberdade e o futuro da internet. Tradução de Cristina Yamagami. São Paulo: Boitempo, 2013.

BARLOW, John Perry. **A Declaration of the Independence of Cyberspace.** Davos: Internet, 1996. Disponível em: https://www.eff.org/cyberspace-independence. Acesso em: 07 ago. 2019.

BAUMAN, Zygmunt et al. Após Snowden: Repensando o Impacto da Vigilância. **Revista Eco Pós**, Rio de Janeiro, v. 18, n. 2, p.8-35, 2015. Disponível em: https://revistas.ufrj.br/index.php/eco_pos/article/view/2660/2225. Acesso em: 20 set. 2019.

BAUMAN, Zygmunt. **Vigilância líquida.** Tradução Carlos Alberto Medeiros. Rio de Janeiro: Editora Zahar, 2014.

BECK, Ulrich. GIDDENS, Anthony. LASH, Scott. **Modernização reflexiva:** política, tradição e estética na ordem social moderna. Tradução de Magda Lopes. São Paulo: Editora da Universidade Estadual Paulista, 1997.

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

BIONI, Bruno Ricardo. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. 2016. 309 f. Dissertação (Mestrado) - Curso de Direito, Universidade de São Paulo, São Paulo, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOBBIO, Norberto; MATTEUCCI, Nicola; PASQUINO, Gianfranco. **Dicionário de política.** Brasília: Editora Universidade de Brasília, 1998.

BOLESINA, Iuri. **O DIREITO À EXTIMIDADE E A SUA TUTELA POR UMA AUTORIDADE LOCAL DE PROTEÇÃO DE DADOS PESSOAIS:** as inter-relações

entre identidade, ciberespaço, privacidade e proteção de dados pessoais em face das intersecções jurídicas entre o público e o privado. 2016. 311 f. Tese (Doutorado) - Curso de Direito, Universidade de Santa Cruz do Sul –, Santa Cruz do Sul, 2016. Disponível em: https://www.unisc.br/images/cursos/stricto/ppgd/teses/2016/Iuri-Bolesina---Tese.pdf. Acesso em: 19 set. 2019.

BOYD, Danah; CRAWFORD, Kate. Critical questions for big data. **Information, Communication & Society**, London, p.662-679, 10 maio 2012. Disponível em: https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf. Acesso em: 15 fev. 2020.

BRASIL. Constituição (1988). **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. Brasília, 05 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 06 ago. 2019.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Brasília, 12 set. 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 06 ago. 2019.

BRASIL. Lei nº 10406, de 10 de janeiro de 2002. **Institui o Código Civil**. Brasília, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 06 ago. 2019.

BRASIL. Lei nº 12.414, de 09 de junho de 2011. **Disciplina A Formação e Consulta a Bancos de Dados com Informações de Adimplemento, de Pessoas Naturais ou de Pessoas Jurídicas, Para Formação de Histórico de Crédito.** 2011a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm>. Acesso em: 15 fev. 2020.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. **Regula O Acesso A Informações Previsto no inciso XXXIII do Art. 5º, no inciso II do § 3º do Art. 37 e no § 2º do Art. 216 da Constituição Federal; Altera A Lei Nº 8.112, de 11 de dezembro de 1990; Revoga A Lei Nº 11.111, de 5 de maio de 2005, e Dispositivos da Lei Nº 8.159, de 8 de Janeiro de 1991; e Dá Outras Providências.** 2011b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 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**. Brasília, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 ago. 2019.

BRASIL. Lei nº 13853, de 08 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. Brasília, 09 jul. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 06 ago. 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 06 ago. 2019.

BRASIL. Proposta de emenda à Constituição nº 17/2019, de 2019. Brasília, 12 mar. 2019. Disponível em: https://legis.senado.leg.br/sdleg-

getter/documento?dm=7924709&ts=1571776978885&disposition=inline. Acesso em: 15 fev. 2020.

CASTELLS, Manuel. **A sociedade em rede –** (A era da informação: economia, sociedade e cultura). V. 1. 3. ed.., São Paulo: Paz e Terra, 2000.

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

2010CASTELLS, Manuel. **Comunicación y Poder.** Alianza Editorial. 2009.

CODING RIGHTS. **DADOS E ELEIÇÕES 2018:** DADOS PESSOAIS E INFLUÊNCIA POLÍTICA. Brasil: Coding Rights, 2018. Disponível em: https://www.codingrights.org/wp-content/uploads/2018/11/Report_DataElections_PT_EN.pdf. Acesso em: 20 ago. 2019.

COMISSÃO EUROPEIA. **C (2012) 5704**: DECISÃO DE EXECUÇÃO DA COMISSÃO de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Bruxelas, 2012. Disponível em: https://op.europa.eu/et/publication-detail/-/publication/d3dd96fc-ee04-11e1-8e28-01aa75ed71a1/language-pt. Acesso em: 10 mar. 2020.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos Humanos**. ROMA, 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 15 fev. 2020.

CONSELHO DA EUROPA. Convenção nº Convenção 108 - 1981, de 20 de janeiro de 1981. **CONVENÇÃO PARA A PROTECÇÃO DAS PESSOAS RELATIVAMENTE AO TRATAMENTO AUTOMATIZADO DE DADOS DE CARÁCTER PESSOAL**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 06 ago. 2019.

DALLA FAVERA, Rafaela Bolson. **Surveillance como violadora de direitos humanos:** o tratamento jurídico do tema nos Estados Unidos e no Brasil; a partir do caso Edward Snowden. 2018. 162 f. Dissertação (Mestrado) - Curso de Direito, Centro de Ciências Sociais e Humanas, Universidade Federal de Santa Maria, Santa Maria, 2018.

DELEUZE, Gilles. Post-scriptum sobre as sociedades de controle. In: DELEUZE, Gilles. **Conversações.** São Paulo: Editora 34, 1992. p. 219-226.

DIETER, Maurício Stegemann. **Política Criminal Atuarial:** A Criminologia do fim da história. 2012. 309 f. Tese (Doutorado) - Curso de Direito, Universidade Federal do Paraná, Curitiba, 2012. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/28416/R%20-%20T%20-%20MAURICIO%20STEGEMANN%20DIETER.pdf?sequence=1. Acesso em: 15 fev. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Chapecó, p.91-98, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 15 fev. 2020.

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

DONEDA, Danilo. Um Código para a proteção de dados pessoais na Itália. **Revista Trimestral de Direito Civil: Rtdc**, Rio de Janeiro, p.1-16, 2003. Disponível em:

https://egov.ufsc.br/portal/conteudo/um-c%C3%B3digo-para-prote%C3%A7%C3%A3o-de-dados-pessoais-na-it%C3%A1lia. Acesso em: 15 fev. 2020. DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** 2011.

DONEDA, Danilo; MENDES, Laura Schertel. Um perfil da nova Lei Geral de Proteção de Dados brasileira. *In*: BELLI, Luca; CAVALLI, Olga (Org.). **Governança e regulações da Internet na América Latina:** análise sobre infraestrutura, privacidade, cibersegurança e evoluções tecnológicas em homenagem aos dez anos da South School on Internet Governance. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2019. 556 p. Disponível em: http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27164/Governan%E7a%20e%20regula%E7%F5es%20da%20internet%20na%20Am%E9rica%20Latina.pdf?sequence=3. Acesso em: 20 ago. 2019.

DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 369-384.

ELLUL, Jacques. **A técnica e o desafio do século.** Paz e Terra, 1955.

EUROPEAN COMMISSION. **GDPR IN NUMBERS:** #HAPPYBIRTHDAYGDPR. Europa, 2019. Disponível em: https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf. Acesso em: 15 fev. 2020.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Data protection in the European Union:** the role of National Data Protection Authorities. Luxemburgo: Publications Office of the European Union, 2010. 56 p. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf. Acesso em: 15 fev. 2020.

FEDERAL TRADE COMMISSION. FTC's $5 billion Facebook settlement: Record-breaking and history-making. **Federal Trade Commission.** Washington, p. 1-1. 24 jul. 2019a. Disponível em: https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history. Acesso em: 17 fev. 2020.

FEDERAL TRADE COMMISSION. FTC sues Cambridge Analytica for deceptive claims about consumers' personal information. **Federal Trade Commission.** Washington, p. 1-1. 24 jul. 2019b. Disponível em: https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftc-sues-cambridge-analytica-deceptive-claims-about.. Acesso em: 15 fev. 2020.

FEDERAL TRADE COMMISSION (United States). **STIPULATED ORDER FOR CIVIL PENALTY, MONETARY JUDGMENT, AND INJUNCTIVE RELIEF:** Case No. 19-cv-2184. District Of Columbia, 2019c. 31 p. UNITED STATES OF AMERICA, Plaintiff v. FACEBOOK, Inc., a corporation, Defendant. Disponível em: https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf. Acesso em: 15 fev. 2020.

FERREIRA, Manuel. **O Regulamento Geral Sobre a Protecção de Dados:** aspectos legais e organizativos de governança nas organizações. Aspectos legais e organizativos de governança nas organizações. 2018. 103 f. Dissertação (Mestrado) - Curso de Direito e Segurança, Direito, Universidade Nova de Lisboa, Lisboa, 2018. Disponível em: https://run.unl.pt/bitstream/10362/54953/1/ManuelFerreira_2018.pdf. Acesso em: 03 mar. 2020.

FORTES, Vinícius Borges. **O direito fundamental à privacidade:** uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. 2015. 225 f. Tese (Doutorado) - Curso de Direito, Universidade Estácio de Sá, Rio de Janeiro, 2015. Disponível em: https://portal.estacio.br/media/922618/ok-vinicius-borges-fortes.pdf. Acesso em: 07 ago. 2019.

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

FOUCAULT, Michel. **Nascimento da Biopolítica:** Curso dado no Collège de France (1978-1979). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. **Vigiar e Punir:** nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis, RJ: Vozes, 2013.

FRYDMAN, Benoit. **Petit manuel pratique de droit global.** Bruxelas: Académie royale de Belgique, 2014.

GETSCHKO, Demi. NETMundial e o Marco Civil: a Necessidade de Ambos. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 101-106.

GIDDENS, Anthony. **As consequências da modernidade.** Tradução de Raul Fiker. São Paulo: Editora UNESP, 1991.

GONÇALVES, Maria Eduarda. **Direito da Informação:** Novos direitos e formas de regulação na sociedade da informação. Coimbra: Livraria Almedina, 2003.

GREENLEAF, Graham. Data Privacy Authorities (DPAS) 2017: Growing Significance of Global Networks. **Privacy Laws & Business International Report**, Sydney, p.1-7, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993186##. Acesso em: 15 fev. 2020.

GUTIERREZ, Andriei. Capítulo IX - Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de dados Pessoais e da Privacidade. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lgpd**: Lei Geral de Proteção de Dados comentada, São Paulo: Thomson Reuters Brasil, 2019, p.387-402.

KURBALIJA, Jovan. **Uma introdução à governança na internet.** São Paulo: Comitê Gestor da Internet no Brasil, 2016. Disponível em: http://www.cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf. Acesso em 18 de agosto de 2019.

HOUSE OF COMMONS. **Disinformation and 'fake news':** Final Report. London, 2019. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>. Acesso em: 15 fev. 2020.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **AÇÃO CIVIL PÚBLICA:** COM PEDIDO DE TUTELA DE URGÊNCIA. São Paulo: S.i, 2018. 55 p. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 15 fev. 2020.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Autoridades de proteção de dados para a américa latina:** Um estudo dos modelos institucionais da Argentina,

Colômbia e Uruguai. São Paulo, 2019. 59 p. Disponível em: https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina. Acesso em: 15 fev. 2020.

INSTITUTO DE TECNOLOGIA & SOCIEDADE DO RIO. **Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais.** Rio de Janeiro: Instituto de Tecnologia & Sociedade do Rio, 3018. 43 p. Disponível em: <https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>. Acesso em: 15 fev. 2020.

INTERNACIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS. **Counting on Commissioners:** High level results of the ICDPPC Census 2017. Hong Kong, 2017. 53 p. Disponível em: https://globalprivacyassembly.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf. Acesso em: 15 fev. 2020.

LAFONTAINE, Céline. **O Império Cibernético:** Das máquinas de pensar ao pensamento máquina. Tradução de Pedro Filipe Henriques. Lisboa: Instituto Piaget, 2007.

LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** São Paulo: Atlas, 2003.

LASH, Scott. **Crítica de la información.** Tradução de Horacio Pons. Buenos Aires: Amorrortu, 2005.

LEMOS, Ronaldo. Uma Breve História da Criação do Marco Civil. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 79-100.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2011.

LIMA, Cíntia Rosa Pereira; BIONI, Bruno Ricardo. A Proteção dos Dados Pessoais na Fase de Coleta: Apontamentos sobre a Adjetivação do Consentimento Implementada pelo Artigo 7, Incisos VIII e IX, do Marco Civil da Internet a Partir da *Human Computer Interaction e da Privacy By Deafult. In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 263-290.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção de dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LUCCA, Newton de; LIMA, Cíntia Rosa Pereira de. *In*: LIMA, Cíntia Rosa Pereira de. Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. **Comentários à Lei Geral de Proteção de Dados**: Lei n. 13.709/2018, São Paulo: Almedina, 2020, p.373-389.

LUCCA, Newton de. Marco Civil da Internet – uma Visão Panorâmica dos Principais Aspectos Relativos às suas Disposições Preliminares. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 23-78.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, [s.l.], v. 1, n. 2, p.205395171454186-13, 9 jul. 2014. SAGE Publications. http://dx.doi.org/10.1177/2053951714541861. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2053951714541861. Acesso em: 15 fev. 2020.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: Fgv Editora, 2018. 192 p. Disponível em: http://eduardomagrani.com/livro-internet-da-coisas-2018/. Acesso em: 08 ago. 2019.

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

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data*. **Revista Eletrônica do Curso de Direito**, Santa Maria, v. 14, n. 3, p.1-27, 2019. Disponível em: https://periodicos.ufsm.br/revistadireito/article/view/41708. Acesso em: 06 mar. 2020.

MENDES, Laura Schertel. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Revista Panorama Setorial da Internet**, São Paulo, p.1-6, jul. 2019. Disponível em: <https://www.cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf>. Acesso em: 07 ago. 2019.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na Sociedade de Consumo. 2008. 158 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Brasília, Brasília, 2008. Disponível em: https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf. Acesso em: 15 fev. 2020.

MENEZES NETO, Elias Jacob de. **Surveillance, Democracia e Direitos Humanos:** os limites do Estado na Era do Big Data. 2016. 291 f. Tese (Doutorado) - Curso de Direito, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2016. Disponível em: http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/5530/Elias%20Jacob%20de%20Menezes%20Neto_.pdf?sequence=1&isAllowed=y. Acesso em: 07 ago. 2019.

MOROZOV, Evgeny. O perigo da publicidade baseada em emoções. **Uol**. 09 dez. 2013. Disponível em: https://www1.folha.uol.com.br/paywall/login.shtml?https://www1.folha.uol.com.br/colunas/evgenymorozov/2013/12/1381821-o-perigo-da-publicidade-baseada-em-emocoes.shtml. Acesso em: 15 fev. 2020.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos Fundamentais**, Vitória, v. 19, n. 3, p.159-180, 2018. Disponível em: http://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603/pdf. Acesso em: 09 mar. 2020.

NASCIMENTO, Valéria Ribas do. Neoconstitucionalismo e ciberdemocracia: desafios para implementação da cibercidadania na perspectiva de Pérez Luño. **Revista de Informação Legislativa**, Brasília, n. 194, p.89-106, 2012. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/496926/RIL194.pdf?isAllowed=y. Acesso em: 18 dez. 2019.

OLHAR DIGITAL. Estudo faz alerta sobre algoritmo médico racista usado nos EUA. 28 out. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/estudo-faz-alerta-sobre-algoritmo-medico-racista-usado-nos-eua/92156. Acesso em: 15 fev. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Americana de Direitos Humanos**. San José da Costa Rica, 1969. Disponível em: https://www.cidh.oas.org/Basicos/Portugues/c.Convencao_Americana.htm. Acesso em: 15 fev. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Declaração Americana dos Direitos e Deveres do Homem**. BOGOTÁ, 1948. Disponível em:

https://www.cidh.oas.org/Basicos/Portugues/b.Declaracao_Americana.htm. Acesso em: 15 fev. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. PARIS, 10 dez. 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/por.pdf. Acesso em: 15 fev. 2020.

PÉREZ LUÑO, Antonio-Enrique. **? Ciberciudadani@ o ciudadani@.com?** Barcelona: Gedisa, 2003.

PÉREZ LUÑO, Antonio-Enrique. Internet y los derechos humanos. **Derecho y Conocimiento:** anuario jurídico sobre la sociedad de la información y del conocimiento. Huelva, v. 2, p.101-121, 2002. Disponível em: http://rabida.uhu.es/dspace/bitstream/handle/10272/2550/b15616630.pdf?sequence=1. Acesso em: 07 ago. 2019.

PÉREZ LUÑO, Antonio-Enrique. Las generaciones de derechos humanos. **Revista Direitos Emergentes na Sociedade Global**, Santa Maria, v. 2, n. 1, p.136-196, 2013. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/10183/pdf_1#.XUpquuhKjIU. Acesso em: 07 ago. 2019.

PÉREZ LUÑO, Antonio-Enrique. La tutela de la libertad informática en la sociedad globalizada. **Isegoría**, [s.l.], n. 22, p.59-68, 30 set. 2000. Editorial CSIC. http://dx.doi.org/10.3989/isegoria.2000.i22.521. Disponível em: http://isegoria.revistas.csic.es/index.php/isegoria/article/view/521/521. Acesso em: 18 dez. 2019.

PÉREZ LUÑO, Antonio-Enrique. La universalidad de los Derechos Humanos. **Derecho y Cambio Social**, Lima, p.95-110, 2007. Disponível em: http://www.derechoycambiosocial.com/revista009/derechos%20humanos.htm. Acesso em: 15 fev. 2020.

PROVIEW, Thomson Reuters. **GUÍA PRÁCTICA PARA LA GESTIÓN DE LA PROTECCIÓN DE DATOS EN LA EMPRESA.** Spain: Editorial Arazandi, 2018.

REZENDE, Pedro Antonio Dourado de. Como entender as denúncias de vigilantismo global?. **Politics**, Rio de Janeiro, p.3-8, out. 2013. Mensal.

RODOTÀ, Stefano. **Iperdemocrazia:** Come cambia la sovranità democrática com il web. Bari: Laterza, 2013.

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

RUARO, Regina Linden; GLITZ, Gabriela Pandolfo Coelho. Panorama geral da Lei Geral de Proteção de Dados pessoais no Brasil e a inspiração no Regulamento Geral de Proteção de dados pessoais europeu. **Revista de Estudos e Pesquisas Avançadas do Terceiro Setor**, Brasil, p.340-356, 2019. Disponível em: https://bdtd.ucb.br/index.php/REPATS/article/view/11545/pdf. Acesso em: 10 mar. 2020.

SANTOS, Boaventura de Sousa. **Para um novo senso comum:** A ciência e a política na transição paradigmática. São Paulo: Cortez, 2002.

SARLET, Ingo. **Curso de direito constitucional.** São Paulo: Saraiva, 2015.

SILVA, Rosane Leal da. Cultura ciberlibertária x regulação da internet. **Revista Brasileira de Estudos Constitucionais - RBEC**: A corregulação como modelo capaz de harmonizar este conflito. Belo Horizonte, p.279-311, 2012.

SCHUTZ, Philip. **Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective.** 2017.

SNYDER, Timothy. What Turing Told Us About the Digital Threat to a Human Future. **The New York Review Of Books**, New York, maio 2019. Disponível em: https://www.nybooks.com/daily/2019/05/06/what-turing-told-us-about-the-digital-threat-to-a-human-future/. Acesso em: 07 ago. 2019.

U.S. Department of Justice. **Report On The Investigation Into Russian Interference In The 2016 Presidential Election.** Washington, 2019. 448 p. Disponível em: https://www.justice.gov/storage/report.pdf. Acesso em: 15 fev. 2020.

UNESCO. **TIC para o desenvolvimento sustentável:** Recomendações de políticas públicas que garantem direitos. Montevidéu: Cetic.br/nic.br, 2019. 80 p. Disponível em: https://cetic.br/media/docs/publicacoes/8/14582020190716-tic-para-o-desenvolvimento-sustentavel.pdf. Acesso em: 07 ago. 2019.

UNIÃO EUROPEIA. Carta nº (2000/C 364/01), de 18 de dezembro de 2000. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. Disponível em: https://www.cnpd.pt/bin/legis/internacional/CARTAFUNDAMENTAL.pdf. Acesso em: 06 ago. 2019.

UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados**. Disponível em: https://eur-lex.europa.eu/eli/dir/1995/46/oj. Acesso em: 06 ago. 2019.

UNIÃO EUROPEIA. **Regulamento nº 2016/679, de 27 de abril de 2016. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt. Acesso em: 06 ago. 2019.

UNIÃO EUROPEIA. **Regulamento (ue) 2018/1725 do Parlamento Europeu e do Conselho de 23 de outubro de 2018 Relativo à Proteção das Pessoas Singulares no Que Diz Respeito Ao Tratamento de Dados Pessoais Pelas Instituições e Pelos órgãos e Organismos da União e à Livre Circulação Desses Dados, e Que Revoga O Regulamento (ce) N.o 45/2001 e A Decisão N.o 1247/2002/ce**. Disponível em: https://europass.cedefop.europa.eu/sites/default/files/regulation-pt.pdf. Acesso em: 10 mar. 2020.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de Abril de 2016 Relativa à Proteção das Pessoas Singulares no Que Diz Respeito Ao Tratamento de Dados Pessoais Pelas Autoridades Competentes Para Efeitos de Prevenção, Investigação, Detecção Ou Repressão de Infrações Penais Ou Execução de Sanções Penais, e à Livre Circulação Desses Dados, e Que Revoga A Decisão-quadro 2008/977/jai do Conselho**. BRUXELAS, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680. Acesso em: 15 fev. 2020.

UNIÃO EUROPEIA. **Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016 Relativa à Utilização dos Dados dos Registos de Identificação dos Passageiros (pnr) Para Efeitos de Prevenção, Deteção, Investigação e Repressão das Infrações Terroristas e da Criminalidade Grave**. BRUXELAS, 04 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0681&from=LV. Acesso em: 15 fev. 2020.

UNIÃO EUROPEIA. **Tratado de Lisboa**. 2007. Disponível em: https://www.parlamento.pt/europa/Documents/Tratado_Versao_Consolidada.pdf. Acesso em: 15 fev. 2020.

UNIÃO EUROPEIA. **Tratado sobre o Funcionamento da União Europeia**. 2009. Disponível em: https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF. Acesso em: 15 fev. 2020.

UNIÃO EUROPEIA. **Tratado que Estabelece Uma Constituição para a Europa**. 2004. Disponível em: https://europa.eu/european-union/sites/europaeu/files/docs/body/treaty_establishing_a_constitution_for_europe_pt.pdf. Acesso em: 15 fev. 2020.

VAINZOF, Rony. Capítulo I – Disposições Preliminares. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lgpd**: Lei Geral de Proteção de Dados comentada, São Paulo: Thomson Reuters Brasil, 2019, p.19-178.

VASCONCELOS, Beto; PAULA, Felipe de. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. A autoridade nacional de proteção de dados: origem, avanços e pontos críticos. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro.**, São Paulo: Thomson Reuters Brasil, 2019, p.717-740.

VIRILIO, Paul. **A arte do motor.** Tradução de Paulo Roberto Pires. São Paulo: Estação Liberdade, 1996a.

VIRILIO, Paul. **El Cibermundo, la política de lo peor.** Madrid: Ediciones Cátedra, 1997.

VIRILIO, Paul. **Guerra e cinema.** Tradução de Paulo Roberto Pires. São Paulo: Boitempo, 2005.

VIRILIO, Paul. **La bombe informatique.** Paris: Éditions Galilée, 1998.

VIRILIO, Paul. **Velocidade e política.** São Paulo: Estação Liberdade, 1996b.

WARREN, Samuel. BRANDEIS, Louis. The Right to Privacy. Havard Law Review. 1890. Disponível em: https://www.jstor.org/stable/1321160?seq=2#metadata_info_tab_contents. Acesso em: 07 ago. 2019.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? **I Encontro da rede de Pesquisa em Governança da Internet – REDE 2017.** São Paulo, 2018. p. 175. Disponível em: http://redegovernanca.net.br/public/conferences/1/anais/Anais_REDE_2017-1.pdf. Acesso em: 23 mar. 2019.

ZANATTA, Rafael A. F. A proteção de dados pessoais entre leis, códigos e programação: os limites do Marco Civil da Internet. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I:** Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p.447-469.