SAMUEL SAMPAIO EVANGELISTA

CONSTITUCIONALISMO DIGITAL: UMA ANÁLISE SOBRE O ESTADO E O DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS

Trabalho realizado sob orientação do
Professor Doutor Gustavo Gramaxo Rozeira

SETEMBRO 2021

SAMUEL SAMPAIO EVANGELISTA

CONSTITUCIONALISMO DIGITAL: UMA ANÁLISE SOBRE O ESTADO E O DIREITO FUNDAMENTAL DA PROTEÇÃO DE DADOS

Dissertação de Mestrado em
Direito Público e Ciências Jurídico-Publicísticas

Tese defendida em provas públicas na Universidade Lusófona do Porto no dia 10 de setembro de 2021, perante o júri seguinte:
Presidente: Prof.ª. Doutora Maria do Rosário Pereira Cardoso dos Anjos (Professora Associada da Universidade Lusófona do Porto);
Arguente: Prof. Doutor Hugo Flores da Silva (Professor Convidado equiparado a Professor Auxiliar da Universidade do Minho);
Orientador: Prof. Doutor Gustavo Jorge Gramaxo Rozeira (Professor Auxiliar da Universidade Lusófona do Porto).

SETEMBRO 2021

AGRADECIMENTOS

Sou grato a todos os professores que contribuíram com a minha trajetória acadêmica, agradeço a todos os professores, por exigirem de mim muito mais do que eu imaginava ser capaz de fazer. Manifesto aqui minha gratidão eterna por compartilharem sua sabedoria, o seu tempo e sua experiência.

Agradeço à universidade, por me proporcionar um ambiente criativo para os estudos. Sou grato à cada membro do corpo docente, à direção e a administração dessa instituição de ensino que, ao longo de minha formação neste curso mestrado, ofereceu um ambiente de estudo motivador e repleto de oportunidades, desde o pessoal do administrativo até o coordenador do curso, que de alguma forma contribuíram para a realização deste trabalho.

RESUMO

Este projeto dissertativo tem como escopo analisar os novos aspectos do constitucionalismo digital e suas novas formas nas diversas visões de estados nacionais. Esses entes têm buscado cada vez mais estreitar a harmonia entre seus ordenamentos jurídicos para tal tema, como também este projeto busca fomentar o debate sobre um dos mais recentes temas no âmbito do Direito Constitucional, o qual busca observar o real impacto que as constituições, legislações de direitos fundamentais e civis, posicionamentos de entidades de caráter internacionais e proposituras legislativas desempenham sobre a proteção de direitos fundamentais no ciberespaço. É evidente que as relações sociais diante das novas tendencias apresentadas pela pluralização do acesso à internet expandem intensamente a capacidade interpretativa dos Tribunais Constitucionais perante os arrojos de eventuais riscos a garantias constitucionais fundamentais. Frente a tal fato, nos últimos anos o debate dentre os membros da comunidade jurídica fomentou diversas investigações que buscaram incansavelmente à identificação de regras e dispositivos normativos legais de espectros gerais de direitos, além de códigos de governança e logicamente as limitações e as regulamentações dos poderes públicos e privados na internet. A própria dimensão objetiva de direitos fundamentais, como os de liberdade de expressão, de participação política, e mesmo de privacidade passa a ser permeada por aspectos técnicos das novas plataformas digitais. É inegável que em nossos dias, a internet pode não só modificar o contexto factual de uma determinada tecnologia, como também levantar teses sobre como a Constituição a ela se justapõe, buscando também analisar a efetividade real de garantias constitucionais além de valores e direito fundamentais na contemporaneidade, examinando-se também, de quais maneiras o constitucionalismo digital e os avanços das novas tecnologias podem cooperar para uma nova forma de proteger informações e dados sensíveis públicos e privados, fortalecer o exercício da cidadania através da vigilância e informação constante dos setores públicos e privados para garantir um meio social que venha a refletir os melhores valores constitucionais.

Descritores: Constitucionalismo Digital; Plataformas Digitais; Direito Fundamentais e Proteção de Dados.

ABSTRACT

This dissertation project aims to analyze the new aspects of digital constitutionalism and its new forms in the different visions of national states. These entities have increasingly sought to strengthen harmony between their legal systems for this topic, as well as this project seeks to foster debate on one of the most recent issues in the scope of Constitutional Law, which seeks to observe the real impact that constitutions, legislations of fundamental and civil rights, positions of international entities and legislative proposals play on the protection of fundamental rights in cyberspace. It is evident that social relations in the face of new trends presented by the pluralization of internet access intensely expand the interpretative capacity of the Constitutional Courts in face of the boldness of possible risks to fundamental constitutional guarantees. Faced with this fact, in recent years the debate among members of the legal community has fostered several investigations that have relentlessly sought to identify rules and legal normative devices of general spectrum of rights, in addition to governance codes and, of course, the limitations and regulations of the powers. public and private on the internet. The very objective dimension of fundamental rights, such as freedom of expression, political participation, and even privacy, becomes permeated by technical aspects of new digital platforms. It is undeniable that nowadays, the internet can not only modify the factual context of a given technology, but also raise thesis on how the Constitution is juxtaposed to it, also seeking to analyze the real effectiveness of constitutional guarantees in addition to fundamental values and rights in contemporaneity, also examining in what ways digital constitutionalism and the advances of new technologies can cooperate for a new way of protecting public and private sensitive information and data, strengthening the exercise of citizenship through constant surveillance and information from the public and to ensure a social environment that reflects the best constitutional values.

Descriptors: Digital Constitutionalism; Digital Platforms; Fundamental Law and Data Protection.

SUMÁRIO

Constitucionalismo digital: Uma análise sobre o estado e o direito fundamental da proteção de dados

Samuel Sampaio Evangelista, Pós-Graduado (Universidade de Fortaleza), Mestrando em Ciências jurídico-publicísticas na Faculdade de Direito e Ciência Política da Universidade Lusófona do Porto, Coordenador do Grupo de Trabalho de Defesas Cibernéticas Nacionais do Grupo de Estudos e Pesquisas em Segurança Internacional do Instituto de Relações Internacionais da Universidade de Brasília (GEPSI), Pesquisador do Laboratório de Simulações e Cenários (LSC) vinculado à Superintendência de Pesquisa e Pós-graduação (SPP) da Escola de Guerra Naval (EGN) da Marinha do Brasil (MB) e demais agências do Estado brasileiro.

1. INTRODUÇÃO

A digitalização global, o compartilhamento internacional de dados e as tecnologias emergentes de processamento de dados ensejam novos desafios à proteção de dados e exigem uma análise comparativa abrangente do papel da proteção de dados nas leis constitucionais como ressalta Rodotà (2008).

Em um ambiente favorável ao crescimento de uma forte indústria de processamento de dados, os interesses do mercado global levam a proteção de dados a se tornar um desafio universal. Neste caminho, constituições e jurisprudência do continente europeu e americano são levadas em consideração pelo desenvolvimento de normas e estudos neste campo nos últimos anos (Doneda, 2018).

Os mecanismos constitucionais de proteção de dados em certos países, como Canadá, Brasil e Estados Unidos (EUA), recebem muita atenção devido à forte relação entre proteção de dados e privacidade em suas jurisdições. Ásia, América do Sul e Europa como observado pelo trabalho de Doneda (2011) ganham atenção como regiões de alto desenvolvimento de estudo neste campo acadêmico.

A elaboração do desenvolvimento da proteção de informações e dados em vários países e regiões do mundo, de acordo com sua progressão oportuna, seguida de uma exposição de seu conteúdo de maneira analítica ao relacionamento multifacetado entre proteção de dados e privacidade pode ser abordado de maneiras diferentes (Doneda, 2019).

A abordagem significativa de Doneda (2019) é contemplar a proteção de dados como uma faceta do direito na proteção de informações e dos dados dos membros da sociedade, com diferentes elementos da lei de proteção de informações e documentações sendo justificados com base em preocupações com a segurança da sociedade assim como da individualidade da privacidade.

Esta abordagem ainda sustenta que a proteção e a privacidade dos dados podem ser consideradas ferramentas complementares, servindo para apoiar o autodesenvolvimento individual, como um componente conceitual necessário da dignidade humana, a base dos direitos fundamentais e constitucionais dos indivíduos e também, a proteção de informações e dados pode ser abordada como um direito significante, que cumpre várias funções, incluindo, razões de segurança nacional e bem estar dos cidadãos amparados pelos dispositivos constitucionais em vigência dentro do ordenamento jurídico que vigora compreendido em suas fronteiras físicas que também se embaralham com as fronteiras digitais existentes.

Os dados podem ser definidos em um sentido amplo como material para fins de análise. As informações geralmente se referem aos resultados da análise de dados assim como de informações através da interpretação do agente governamental que o interpreta ou o guarda (Gillespie, 2017).

Devido ao potencial dos dados de fornecer uma grande quantidade de informações diversas sobre de quem os dados pertencem, não são principalmente os dados que precisam ser protegidos, mas o titular dos dados. A proteção de dados pessoais e sensíveis visa proteger as pessoas de quem os dados se originam, em particular proteger seus direitos e liberdades, que podem ser comprometidos como resultado de seus elementos informacionais e de registros de comportamento e atividades diversas serem aplicados de maneiras diferentes (Bassini, 2019).

Para que informações ou dados se qualifiquem como sensíveis ou de alto valor, eles podem estar relacionados a uma pessoa que já está identificada, a uma instituição ou agencia governamental identificável, com base nesses dados (Guidi, 2018). Logo o direito à proteção da informação e dos dados pessoais é um fenômeno relativamente novo no direito constitucional.

Em seu recente surgimento, conforme ressalta Guidi (2018), as abordagens atuais e recentes o rotulam como um direito autônomo, e sua distinção, muitas vezes pouco esclarecedora, sobre o direito da privacidade, indo inclusive até as legislações

complementares, regulamentos e garantias da segurança nacional de um país no qual ambas ainda sujeitas a discussões contínuas sobre seus conceitos.

Ocorre que o direito à proteção de dados sensíveis ou de determinadas classificações é de importante e de significativo interesse da justiça na busca de originar uma análise sobre essa matéria conexa à constituição teórica-conceitual, não obstante ao ímpeto de conceituar o termo pela ocorrência de ser este um dos neófitos entes conceituais do direito constitucional moderno no nosso atual âmbito jurídico e social (Floridi & Taddeo, 2016).

Na definição constitucional, sejam aquelas que vigoram em países membros da União Europeia do mesmo modo como aquelas que competem a países do continente Americano, no conceito da essência dos direitos fundamentais, a proteção de dados desempenha um papel crucial. A interpretação dessa noção tem um impacto considerável, não apenas na percepção da essência em outros campos do direito, mas também na doutrina constitucional em geral (Doneda, 2018).

Este trabalho dissertativo busca concentra-se também nas especificidades da noção de essência dos direitos à proteção de dados e informações sensíveis e pessoais, ligados à sua matriz constitucional vislumbrando as legislações gerais de proteção de dados ao redor do mundo.

Após uma análise geral, situando este estudo na noção do quadro da proteção multinível dos direitos fundamentais na Europa e Américas, a pesquisa também aborda outros desafios interpretativos relacionados à essência da jurisprudência no sistema judiciário e nos novos modelos de trabalho de governança pública.

Nesse contexto, também se analisa a importância de "*insights*"[1] nos campos da proteção social de informações e de dados gerais e pessoais, da segurança destes elementos ligado aos dados pessoais e sensíveis para o entendimento constitucional amplo do conceito de sua essência e propõe examinar métodos generalizados para determinar a violação da sua essência na jurisprudência destes direitos fundamentais, nos mais variados sistemas políticos, que estão vindo a estabelecer fundamentos constitucionais para a interpretação dessa noção (Celeste, 2019).

[1] Insight ou entendimento, segundo o Oxford Advanced Learner's Dictionary é a compreensão de uma causa e efeito específicos dentro de um contexto particular. O termo insight pode ter vários significados relacionados: um pedaço de informação o ato ou resultado de compreender a natureza interna das coisas ou de ver intuitivamente uma introspecção. Recuperado em 27 de março de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/insight.

Embora as legislações sobre proteção de dados possam assumir muitas formas, várias abordagens que procuram regular a coleta, o uso e a disseminação de informações pessoais online enfrentam possíveis limitações. Isso porque os estudiosos dividiram-se sobre como a aplicabilidade da regulamentação deve ser proposta na esfera da proteção e segurança de dados.

Em uma linha de pensamento acompanhando Doneda (2018), os dados constituem uma abordagem expansiva a capacidade do governo de regular a atividade virtual de informações e dados importantes sensíveis, que leva a um conflito com o complicado emaranhado de jurisprudência que se desenvolve nesta área.

Recentes violações de dados de alto nível e outras preocupações sobre como terceiros protegem a privacidade de indivíduos na era digital provocaram preocupações em diversas nações sobre proteções legais aos dados eletrônicos. Intrusões intencionais nas redes de computadores governamentais e privadas, além de práticas inadequadas de privacidade e cibersegurança corporativa em que expuseram as informações pessoais de milhões de membros de nossa sociedade a destinatários indesejados (Bioni, 2019). É possível exemplificar tais fatos à medida que mais atividades sociais e econômicas incidem em plataformas on-line, a seriedade sobre o direito à privacidade e da proteção de dados é cada vez mais reconhecida[2] como apontado pela UNCTAD[3].

No entanto, as novas estruturas fornecem um ponto de partida importante e fundamental para garantir que as fortes salvaguardas legais e regulamentares fundamentais sejam implementadas para fornecer estruturas de governança necessárias em nível nacional

[2] O UNCTAD Global Cyberlaw Tracker é o primeiro mapeamento global de leis cibernéticas. Ele rastreia o estado da legislação de comércio eletrônico no campo de transações eletrônicas, proteção ao consumidor, proteção de dados e privacidade e adoção de crimes cibernéticos nos 194 estados membros da UNCTAD. Indica se um determinado país adotou legislação ou não, ou se tem um projeto de lei pendente de adoção. Em alguns casos em que as informações sobre a adoção da legislação de um país não estavam prontamente disponíveis, nenhum dado é indicado. Recuperado em 07 de março de 2019, de https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[3] A Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) foi estabelecida em 1964, em Genebra, Suíça, no contexto das discussões de liberalização do comércio no Acordo Geral de Tarifas e Comércio. É o órgão da Assembleia Geral das Nações Unidas que busca promover integração de países em desenvolvimento na economia mundial e atual como fórum para deliberações intergovernamentais, apoiado por debates com especialistas e intercâmbio de experiências. Também desenvolve pesquisas, análises de políticas e coleta de dados para debates de representantes do governo e especialistas. Recuperado em 07 de março de 2019, de https://unctad.org/.

e global seguindo o pensamento apresentado por Rodotá (2008), antes de ver-se no assunto da exploração de dados por empresas de entres públicos e privados.

Ao mesmo tempo, a conectividade com a Internet aumentou e tomou várias formas nos últimos anos. Agora, os cidadãos comuns transmitem seus dados pessoais e informações particulares na Internet a uma taxa exponencialmente maior do que no passado, e tão logo seus dados são coletados, cultivados e mantidos por um número crescente de intérpretes, que voltados para os mais variados motivos, além de nos bastidores, atuam como criadores, corretores e moderadores de dados (Doneda, 2018).

Como consequência, a garantia, a cibersegurança e a proteção de dados dos cidadãos surgiram como uma questão importante para consideração do direito constitucional dentro do meio público e da organização social nos novos tempos que a tecnologia nos proporciona (Lambach, 2019).

Apesar do aumento do interesse na segurança e proteção de dados, de informações da sociedade, os paradigmas legislativos que regem a cibersegurança e a privacidade dos dados são complexos e técnicos, e conforme observa Bioni (2019) carecem de uniformidade em sua orientação diante do contexto do direito constitucional, com ênfase na área pública, no que diz respeito a proteção e a segurança daqueles a quem as constituições guardam.

Diante da vulnerabilidade causada pela carência da segurança dos dados de seus cidadãos e de processos informatizados de diretivas administrativas e institucionais que se desenvolveram ao longo do século XXI segundo Mattiuzzo (2018), mas esse direito geralmente protege apenas contra invasões do governo e pouco faz para proteger o usuário médio da Internet de possíveis ataques privados.

Estatutos atuais buscam regular, principalmente, certas indústrias e subcategorias de dados e preenchem algumas das lacunas estatutárias ao impor uma ampla proibição contra práticas injustas e enganosas para garantir a segurança e proteção de dados de maneira abrangente (Celeste, 2019).

Buscando um sistema de proteção de dados mais abrangente, alguns governos, como o do estado da Califórnia (EUA) e a União Europeia (UE), promulgaram recentemente leis que regulam quase todas as formas de dados e informações dentro do seu alcance jurisdicional, levando a importância de seu estudo e suas implicações futuras no campo jurídico global (Yilma, 2017).

Como notado na obra de Land (2016), em uma perspectiva de direitos humanos de segurança e proteção aos seus dados e informações, que caracterizam informações

particulares e pessoais dos indivíduos, públicos ou privados devem estar sobre a proteção ofertada pelo direito constitucional de um Estado Democrático de Direito maduro e que acompanha a evolução dos novos tempos.

Conforme será observado ao longo da análise dissertativa, tais diferenças surgem mesmo entre os membros da esfera ocidental, liberal, democrática e não desaparecerá rapidamente. É perceptível a partir do estudo sobre a natureza dos direitos fundamentais, no qual é possível dizer que, no atual contexto social, a importância da segurança e proteção das informações e dos dados pessoais e sensíveis, juntamente com o cuidadoso tratamento com desígnio de que estes dados sejam protegidos é uma maneira de avalizar o caráter basilar de sua estima para a nossa civilização e, em especial, para as sociedades civilizatórias que tem como base jurídica fundamentada no direito constitucional.

Fortalecendo a interpretação como sendo parte da cultura jurídica ligada também a dignidade da pessoa humana, direito este reconhecido como sendo parte fundamental dos valores constitucionais modernos, em que preceitos e direitos fundamentais tais como a proteção dos seus dados, valores, preferencias, particularidades e personalidade estão sendo balizados por entes que devem ser observados e regulados pela ordem jurídica vigente, e como afirmado por Luís Roberto Barroso:

> A dignidade humana é um valor fundamental que informa o conteúdo de diversas normas escritas, ao mesmo tempo em que condiciona a interpretação constitucional como um todo, principalmente quando os direitos fundamentais estão envolvidos (Barroso, p. 51, 2014).

A formulação futura de políticas nacionais e internacionais no campo do direito constitucional sobre este tema terá que se envolver seriamente com nações e culturas fora dessa esfera, superando as diferenças e encarando um outro fator ainda mais temerário que será a falta de um órgão internacional representativo, suficientemente forte e dinâmico, que venha a ter capacidade o suficiente para realizar o trabalho de construir uma ponte buscando conectar e coadunar as diferentes visões de como enxergar estes dados e informações, além de suas diversas funcionalidades e, em especial, o que eles representam sobre aqueles a quem pertencem.

2. O DIREITO A PROTEÇÃO DE DADOS

O conceito atual de dados pessoais que determina o escopo material da segurança e proteção de dados deve ser amplo segundo Bioni (2019), mas deverá se expandir ainda mais e, como resultado, se aplicar a uma gama de situações em crescimento exponencial. Isso se deve às possibilidades embutidas para a interpretação em evolução do próprio conceito, geração e agregação explosiva de informações e dados, bem como avanços na sua devida análise.

Como o ambiente está se aproximando rapidamente no qual, a existência diária, é mediada pela tecnologia da informação, tudo neste ambiente, desde o clima, águas residuais, roteiros de exames, está sendo cada vez mais digitalizado e, literalmente, qualquer dado pode ser plausivelmente considerado pessoal[4].

Dados pessoais representam uma das principais noções da lei de proteção e segurança de informações que determina o escopo material das legislações que versam sobre a proteção de dados. A definição resultante de dados pessoais é ampla, flexível e adaptável ao contexto tecnológico, e também as referências a pessoa identificável e informações relativas a uma pessoa acenam à interpretação sobre o que constitui uma possibilidade relevante de identificação, e uma relação relevante entre as informações e um indivíduo (Bioni, 2019).

Considerando que as diversas leis de proteção de dados adotam um teste de probabilidade razoável de identificação pelo estado gestor dos dados ou por outra pessoa, levando em consideração não a capacidade subjetiva de identificação, mas o estado d artifício tecnológico no momento do processamento destes dados e informações sensíveis (Schwartz & Solove, 2011).

Em uma ampla pesquisa, Bioni (2019), observa que devido à flexibilidade da definição no âmbito das legislações de proteção de dados, e apesar ser um instrumento de harmonização total, tem havido uma divergência significativa na forma como as legislações das nações tem implementado, até agora, a definição de dados pessoais, e uma harmonização completa ainda mais especificamente na seara constitucional, apenas previne os estados nacionais de acrescentarem elementos adicionais às disposições harmonizadas, mas ainda permite decidir os pormenores ou escolher entre as opções que acreditam ser pertinentes.

---

[4] A nova experiência de uma realidade hiperconectada dentro da qual não faz mais sentido perguntar se alguém pode estar *online* ou *offline'* (Luciano Floridi, 'Introdução' em Luciano Floridi (ed.), *The Online Manifesto. Being Human in a Hyperconnected Era* (Springer, 2015).

Tomados em conjunto, esses instrumentos formam um campo de direito e política que tem alcançado considerável maturidade, disseminação e importância normativa ao longo das últimas quatro décadas. Mais de quarenta países já promulgaram legislações, relativamente abrangentes, e normas de segurança e proteção de dados, e estas iniciativas de diversos estados são acrescidas e muitas vezes inspiradas por um grande número de acordos internacionais envolvendo o campo regulatório e um corpo imenso de análise de comentários acadêmicos e questões relevantes a privacidade, segurança e proteção de dados sob uma variedade de perspectivas (Bioni, 2019).

Assim, o cenário global de proteção de dados é extremamente complexo e está bem além do escopo deste trabalho para descrever com precisão todos os seus cantos e recantos. A principal missão destas legislações aqui comentadas é apresentar, brevemente, várias conceituações de diversos países, com suas singularidades regionais e culturais dos ideais e fundamentos do direito constitucional e proteção de dados, para delinear a linha de pensamento internacional e perspectivas legislativas de inúmeros países na área de segurança e proteção de dados e informações, destacando ao mesmo tempo suas principais semelhanças e diferenças (Land, 2016).

Na maior parte, a análise a ser feitas destes tipos de legislações e seus objetivos, conforme a obra de Bioni (2019) é ampla, portanto, sua abordagem quanto a observação científica tende a evitar examinar em detalhes as regras e princípios contidas nos instrumentos em questão, sendo o esforço direcionado, ao invés de resumir padrões regulatórios básicos no cenário global, de segurança e proteção de dados, ter o foco no seu quadro geral.

2.1 Um breve histórico sobre a proteção de dados

Uma discussão séria decolou na década de 1960 sobre as implicações do processamento informatizado de dados pessoais, a privacidade foi invocada como um termo basilar para resumir os amontoados de medos levantados pelo uso de computadores, ou seu eventual mal uso. No entanto, privacidade não foi o único termo invocado neste contexto. Uma variedade de outros conceitos parcialmente sobrepostos também foram invocados, particularmente aqueles de liberdade e autonomia do uso de informações (Pinheiro, 2015).

No entanto, o campo do direito e da política, se cristalizou desde o início as discussões europeias sobre as ameaças relacionadas com a informatização de dados e suas

eventuais regulações, em que têm sido frequentemente descritos utilizando uma nomenclatura que evita referência explícita a privacidade ou tem-se intimamente relacionados, adotando a nomenclatura "proteção de dados", derivada da Termo alemão "*Datenschutz*"[5].

Vários países e regiões apresentam idiossincrasias terminológicas que refletem parcialmente diferentes origens jurisprudenciais para as discussões em causa (Castro, 2005). Na Europa Ocidental, a discussão frequentemente se baseia ali, onde se desenvolveu a jurisprudência sobre a proteção jurídica da personalidade. Por outro lado, o discurso latino-americano no campo tende a girar em torno do conceito de "*habeas data*" em que o significado seria "você deve ter os dados". Este conceito deriva da doutrina do devido processo legal com base no mandado de *habeas corpus*[6].

E seguindo o pensamento de Mattiuzzo (2018), muitos dos conceitos mencionados acima estão sujeitos à instabilidade de definição. O caso mais famoso é a "privacidade". Várias definições do conceito abundam e um longo debate acalorou-se, predominantemente em diversos Circuitos Jurídicos, especialmente aqueles localizados nos Estados Unidos da América, sobre qual definição é a mais correta[7].

Em janeiro de 2012, as legislações de proteção de dados tomaram um novo caminho após a Comissão Europeia, ciente da falta de consenso sobre a segurança e proteção de dados pessoais em todos os países da União Europeia, e considerando o assunto importante, decidiu elaborar um regulamento sobre a matéria. Muitos países membros foram consultados e um

---

[5] "*Datenschutz*", consultar Simitis, S. (ed.), *Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, Baden-Baden*, (6ªed.), 2006.

[6] Guadamuz, A. (2000). Habeas Data: The Latin American Response to Data Protection, *The Journal of Information, Law and Technology*, 2. Recuperado em 02 de junho de 2019, de www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_2/guadamuz; Organização dos Estados Americanos (OEA), Inter-Comissão Jurídica Americana (relator Fried, JT), Direito à Informação: Acesso e Proteção de Informações e Dados Pessoais em Formato Eletrônico, no Relatório Anual da Comissão Jurídica Interamericana, CJI / doc. 45/00. Enquanto o conceito tem origem na América do Sul, mas também começou a se estabelecer em partes do Sudeste Asiático. Em 2008, a Suprema Corte das Filipinas adotou formalmente uma "Regra no Mandado de Habeas Data "como regra de tribunal.

[7] Solove, D. (2008). *Understanding Privacy*. Harvard University Press, Cambridge, Massachusetts; Inness, J.C. (1992). Privacy, Intimacy, and Isolation, *Oxford University Press*, New York/Oxford. Privacidade: Law, Ethics and the Rise of Technology, Cornell University Press, Ithaca, Londres 1997.

primeiro esboço do regulamento foi proposto pela Comissão Europeia em novembro de 2013[8].

O texto então começa a ser discutido em 11 de março de 2014 no Parlamento Europeu, que o modifica, e o adota no dia seguinte em primeira leitura. As negociações continuaram rapidamente entre a Comissão Europeia, o Parlamento Europeu e o Conselho da União Europeia, o que levaria ao texto final em 15 de dezembro de 2015[9].

Como constata-se de acordo com Guidi (2018), o procedimento de adoção deste dispositivo legal, como é frequente na União Europeia, durou um longo período durante o qual os diversos atores, sejam eles estados, empresas e cidadãos, puderam participar no processo de criação, contudo para tentar obter um texto equilibrado, em que ao mesmo tempo que protege as pessoas, deixa certa liberdade às empresas e às administrações públicas.

2.2 Principais características direito de proteção de dados

Os direitos de segurança e proteção dos dados permitiu aos cidadãos conhecer e obter informações sobre os seus dados pessoais sujeitos a tratamento; corrigir erros, modificar dados que se revelem imprecisos ou incompletos, apagar dados inadequados ou excessivos; e se opor ao tratamento inadequado como aponta a pesquisa de Guidi (2018). É importante conhecê-los, para evitar que nossos dados e informações pessoais sejam tratados indevidamente.

O momento de grande globalização e difusão de dados vem inspirando os mais novos movimentos e legislações a respeito de tais garantiras jurídicas do tema, que apresentam novas normas abrangentes e a segurança sendo o ponto central, junto aos regulamentos e legislações pertinentes ao tema que buscam dar aos indivíduos muito mais poder sobre seus dados pessoais (Mendonça, 2018).

Questões complexas, como quais informações pessoais são coletadas, como estão sendo usadas, o que acontece quando eles desejam remover o consentimento, proporcionam aos indivíduos mais segurança de seus dados (Lima, 2014). Dentre os principais recursos deste novo conjunto jurídico que afeta indivíduos e empresas está a permissão específica expressa, onde a menos ou até que você dê permissão a um aplicativo ou site para usar suas

[8] Texto apresentado A7-0402 / 2013, 22 de novembro de 2013, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[9] Parlamento Europeu, CRE de 03/11/2014 e 03/12/2014.

informações de uma maneira específica, eles não podem usá-los para nenhuma outra finalidade ou vendê-los a terceiros.

Tem de haver um consentimento claro e afirmativo antes de os dados privados serem processados (Mendonça, 2018). Diversos legisladores manifestam claramente que o silêncio, as caixas pré-marcadas ou a inatividade não constituem consentimento. No futuro, também deve ser tão fácil para uma pessoa retirar o consentimento quanto concede-lo.

Destaca-se ainda os limites do uso de perfis, em que frequentemente, vemos que os dados e informações pessoais são usados automaticamente para acessar e analisar escolhas pessoais, prever o desempenho de uma pessoa no trabalho, situação econômica, saúde, localização, comportamento, solvência, etc. (Elias, 2017).

De acordo com o Regulamento Geral de Proteção de Dados (RGPD)[10], por exemplo, a criação de perfis será permitida com o consentimento da pessoa em questão, quando permitido por lei ou bem como necessário para buscar um contrato e requer intervenção humana. Outro ponto segundo Mattiuzzo (2018) a avultar seria as soluções "*one-stop*" que será extremamente benéfico para as empresas, pois elas terão que lidar com apenas um órgão regulador em vez de 28, tornando mais simples e barato para as empresas fazer negócios na União Europeia.

As informações em linguagem clara e legível também são uma parte primordial das novas legislações, visto o direito dos indivíduos em obter e ler as informações com clareza. Assim, as novas regras vão acabar com as políticas de privacidade de "letras pequenas" e essa informação deve ser dada em linguagem clara e simples antes de qualquer dado ser coletado (Guidi, 2018).

Também se desponta o direito de ser esquecido observando a pesquisa de Castro (2005) em que dar seus dados a alguém não significa que essa pessoa tenha o direito de mantê-los para sempre. O cidadão tem o direito de ser esquecido e poderá pedir a empresas ou plataformas que excluam seus dados.

No entanto, as duas exceções, que são a que não se aplicará a informações cuja guarda seja legalmente obrigatória, como prontuários médicos e que é também um direito pessoal

[10] Texto consolidado; 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 / EC *(Regulamento Geral de Proteção de Dados*). Recuperado em 11 de março de 2019, de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434..

de esquecimento, distinto do Direito de ser esquecido de terceiros, onde os indivíduos podem solicitar que informações desatualizadas ou indesejáveis sobre eles sejam removidas dos motores de busca (Castro, 2005).

Deve haver o direito de ser esquecido, e ter os dados coletados legalmente excluídos sob as instruções do titular dos dados? O que isso significa em um mundo de *'Big Data'*? Excluir dados é fácil, contudo, impedir que reapareçam de outra origem é muito mais difícil como ficou evidente nos apontamentos de Soprana (2018). As novas regras promovem técnicas como a remoção de informações de identificação pessoal onde não são necessárias, a substituição de material de identificação pessoal por identificadores artificiais e de criptografia, além da codificação de mensagens para que apenas aqueles autorizados possam lê-las, para garantir a segurança dos dados pessoais (Guidi, 2018).

Portanto, as novas regras de proteção de dados e de informações não apenas fornecem aos indivíduos e ao estado informações claras e eficazes sobre como seus dados estão sendo usados, mas também dão às empresas e ao estado a oportunidade de inovar e reconquistar a confiança dos cidadãos observando Aieta (2014), que explica por que a proteção e privacidade de dados e informações apresenta-se como uma das questões mais significativas em nossa civilização contemporânea.

Os dados são um dos ativos mais importantes de uma democracia, pois com o crescimento da economia de informações e dados, as empresas encontram um valor enorme na coleta, compartilhamento e uso destes arquivos. A transparência em como as empresas e o estado solicitam consentimento, cumprem suas políticas de privacidade e gerenciam os dados que coletaram é vital para construir confiança e responsabilidade com os cidadãos e os entes estatais e sociais. Muitas democracias aprenderam a importância da proteção dos dados da maneira mais difícil, por meio de falhas de segurança de dados altamente divulgadas (Aieta, 2014).

Segundo Soprana (2018), a privacidade e segurança de dados e informações é o direito de um indivíduo de ser livre de vigilância indesejada. Existir com segurança em seu espaço e expressar livremente suas opiniões a portas fechadas é fundamental para viver em uma sociedade democrática, visto que a privacidade é a base da nossa liberdade, é de suma importância de forma antropológica e sociológica, moldando a personalidade do ser humano, em momentos de reserva e reflexão pessoal.

Apesar dos avanços recentes na legislação e prática de segurança de dados, a privacidade do cidadão é regularmente invadida ou comprometida por empresas e governos.

Isso levou a concepções de que os consumidores por exemplo já perderam a guerra pela privacidade (Soprana, 2018). Embora possa existir proteção de dados sem privacidade de dados, não se pode ter privacidade de dados sem proteção de dados.

A proteção legal das informações também inclui os regulamentos exigidos pelas empresas para proteger os dados, e à medida que mais regulamentações de segurança proteções de dados crescem em todo o mundo, os requisitos e demandas globais de segurança de tais informações e de dados tratados como sensíveis também se expandem e mudam (Soprana, 2018). No entanto, a única constante é que a proteção adequada dos dados é a melhor forma de garantir que as democracias modernas cumpram a lei e garantam a privacidade e segurança das suas informações e de seus membros (Guidi, 2018).

Embora a maioria das pessoas concorde com a importância da segurança privacidade de dados e informações, e todos concordem que a proteção de dados está também no centro da garantia do direito à privacidade como ressalta a pesquisa de Soprana (2018), a própria definição de proteção de dados é notoriamente complicada.

O problema é que as implicações práticas dessas regras são incrivelmente complexas. O Regulamento Geral de Proteção de Dados (RGPD), por exemplo, como grande parte da legislação da União Europeia, procura apresentar um compromisso entre os diferentes sistemas e valores de países variados. Por causa disso, muitos cientistas e gestores de dados que estarão sujeitos à lei acham isso incompreensível e duvidam que a conformidade absoluta seja mesmo possível (Soprana, 2018).

Felizmente, os legisladores reconheceram a importância de haver regulamentação de segurança e privacidade de dados e a necessidade de responsabilizar o estado e as empresas pelos dados do usuário final (Soprana, 2018). As nações agora são obrigadas, dada a natureza da evolução da globalização a passos largos, a determinar quais atos e leis de proteção e privacidade de dados afetam seus cidadãos, por exemplo, você deve saber a origem dos dados, quanto ao país, sua geolocalização, informações de identificação pessoal e a sua metodologia de uso destas informações.

Logo, examinar mais de perto como os regulamentos de proteção e segurança de dados mais recentes afetam cidadãos e estados nacionais diante das mais importantes legislações de privacidade de dados do mundo é de grande necessidade em nossos tempos. A coordenação entre todas as regras e regulamentos díspares é uma tarefa gigantesca. Estar fora de conformidade pode significar multas pesadas e outras penalidades, incluindo ter que parar de realizar negócios ou transações comerciais no país ou região coberta por lei ou

regulamento que vise garantir a integralidade de diversos tipos de informações de cada membro da sociedade (Proxxima, 2018).

Para uma organização global, se deve ter uma política de proteção de dados que esteja em conformidade com o conjunto de regras mais rigorosas, em que o estado assim como a empresa privada enfrenta, ao mesmo tempo que usa uma estrutura de segurança em conformidade que cobre um amplo conjunto de requisitos legais para garantir a devida segurança de informações, sejam elas as que são coletadas e armazenadas, assim como aquelas que estão sendo captadas em tempo real (Celeste, 2019).

2.3 A importância que amparam a proteção de dados como um direito fundamental

Além da incerteza da base legislativa para a sua incorporação, a natureza do direito à proteção de dados tem sido por vezes criticada como sendo necessariamente de natureza processual, na medida em que não representa diretamente qualquer valor ou interesse por si só, e preceitua os procedimentos e métodos para buscar o respeito aos valores incorporados em outros direitos (Rodotá, 2008).

Isso, nos leva a pesquisa de Rodotá (2008) a entendimentos passados em que ao abafar um direito fundamental, visto que o reconhecimento dos direitos de segurança de informações como fundamentais na organização social e que reflete as normas que sustentam uma ordem jurídica moderna, iria ocasionar um dano imaginável, no qual não haveria garantias de prevenir ou punir uma violação comprovada a dados sensíveis de uma nação ou mesmo do cidadão comum, além de não saber como imputar culpa ou penalidade ao autor de tal infração.

Isso é ilustrado pela extensa jurisprudência sobre o direito a um julgamento justo e eficiente, por exemplo, no qual uma violação pode ser encontrada mesmo quando existe o desrespeito a um componente do direito a um julgamento justo, como o direito de interrogar testemunhas ou acesso a um advogado, logo isso não deve ter o impacto perceptível no resultado de um eventual julgamento e nem na garantia da preservação da lei e da ordem social e antropológica (Rodotá, 2008).

Os direitos são reconhecidos como tal porque protegem valores específicos de uma sociedade e, para Catarina Sarmento & Castro (2005), embora as violações dos direitos muitas vezes resultem em danos graves aos requerentes, este não é um componente necessário de uma reivindicação porque uma violação desses direitos é um ataque aos

valores que sustentam o sistema jurídico, e esse é o dano contra o qual a jurisprudência de direitos humanos considera por vezes irreparável. Portanto, é oportuno examinar quais os valores dão a devida importância para que possa sustentar o direito à proteção de dados como um aspecto fundamental da orbita constitucionalista (Castro, 2005).

As assimetrias de poder inerentes à área de proteção de dados, visto as questões relativas ao consentimento e ao conhecimento, conforme mencionado outrora, e, diversas legislações buscam abordar esse fato, definindo o consentimento como qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados, pelos quais, por uma declaração ou por uma ação afirmativa clara, significa concordar com o tratamento de dados pessoais que lhe digam respeito pois qualquer pedido de consentimento deve ser inteligível, acessível e em linguagem clara e simples[11].

O atual cenário jurídico da civilização ocidental associa explicitamente este requisito ao conhecido princípio da transparência. Esta formulação é vista de diversas maneiras como forçosa e aborda o desequilíbrio de poder, na medida em que forçaria a divulgação de informações sobre transferência e uso de dados[12]. É por esta razão que se argumenta que, embora o direito à privacidade possa ser definido como uma ferramenta de opacidade que estabelece limites para o exercício normativo do poder, o direito à proteção de dados é uma ferramenta de transparência, que canaliza o exercício desse poder normativamente aceito dentro do ordenamento jurídico que este esteja vigente (Schwartz & Solove, 2011).

Relacionado ao princípio de transparência está o reconhecimento de que a coleta e o processamento de dados devem ser realizados de forma a evitar efeitos discriminatórios sobre as pessoas com base na raça ou origem étnica, opinião política, religião ou crenças, filiação sindical, estado saúde ou orientação sexual (Castro, 2005).

Para o efeito, o legislador hoje em um mundo plural e cosmopolita estabelece o direito de não estar sujeito a uma decisão baseada exclusivamente em processamento automatizado, incluindo perfis, definido como o uso de dados pessoais para analisar ou prever certos aspectos de uma pessoa, incluindo sua saúde, comportamento, movimentos e preferências pessoais. Além disso, o processamento de dados pessoais, biométricos ou genéticos para fins de identificação de um indivíduo ou revelação de quaisquer características protegidas pelo estado (Soprana, 2018).

---

[11] Lynskey, O. (2014) *Deconstructing data protection:* The 'Added-Value' of a Right to Data Protection in the EU Legal Order. International and Comparative Law Quarterly nº 63.

[12] Schwartz, PM. (2004). *Property, privacy, and personal data.* Harvard Law Review nº 117.

Essas proibições reconhecem que tal processamento pode ter um efeito discriminatório inerente, e a discriminação é um dos danos potenciais hoje constatados em meio a má utilização de coleta indevida de dados[13].

Pode-se argumentar que o direito à proteção de dados protege a vida futura de alguém, na medida em que a coleta de dados não pode causar nenhum dano no momento de sua coleta, mas o potencial de que esses dados possam ser processados em uma data posterior para traçar o perfil ou fazer avaliações sobre a pessoa ou grupos de pessoas em questão. O conhecimento de que os dados podem ser coletados em massa e armazenados para processamento futuro pode ter um efeito estorvante na sociedade (Guidi, 2018).

Outro valor importante de acordo com Castro (2005) é o direito à proteção de informações que resguarda a autonomia do indivíduo, isso fica claro pela continuação da centralidade do consentimento no qual se observa que as pessoas físicas devem ter controle sobre seus próprios dados pessoais. O princípio da autonomia é o enfoque relacionado no consentimento que também estão claramente e fortemente ligados ao conceito de dignidade.

Quando observamos os tribunais alemães que desenvolveram a noção de autodeterminação informacional[14], ela foi concebida como relacionada ao direito constitucional à dignidade. O foco no consentimento no direito à proteção de dados e informações é o que mais se aproxima da chamada teoria da vontade dos direitos, em que a teoria da vontade vê a função dos direitos como sendo a concessão de controle aos detentores de direitos para sujeitar a outros ao dever de respeitar esses direitos, tais como só muito conhecidos os procedimentos de delegação de poderes, curadorias ou procurações (Rodotá, 2008).

Como observa-se nos últimos anos com os adventos de novas tecnologias, redes sociais e novas ferramentas utilitárias tecnológicas que utilizam dados sensíveis, os indivíduos muitas vezes não estão cientes nem controlam o que acontece com suas informações e com seus dados pessoais, portanto, não conseguem exercer os seus direitos de forma eficaz (Mendonça, 2018). Para esse fim, combina-se a ênfase na autonomia e consentimento com um foco paralelo nas funções dos controladores de dados,

---

[13] *Intelligence and Security Committee of Parliament. Privacy and Security: A Modern and Transparent Legal Framework*. (2015). Recuperado em 25 de maio de 2019, de http://isc.independent.gov.uk/committee-reports/special-reports.

[14] DeHert & Gutwirth (2006). *Privacy, data protection and law enforcement*. Privacy and the Criminal Law. Ed. Oxford, UK.

independentemente de os titulares dos dados terem tomado medidas positivas para fazer cumprir essas obrigações.

Este aspecto se encaixa mais de perto com a teoria do interesse dos direitos, que vê a função dos direitos humanos como a imposição de um dever positivo aos atores de respeitar os interesses dos outros, independentemente de o detentor dos direitos reivindicar esse dever, levando estes aspectos a muitas cartas constitucionais (Rodotá, 2008).

De fato, a comunidade cientifica, visto o argumento de Mendonça (2018) levanta o fato de que o foco nos controladores de dados em diversos modelos legislativos pelo mundo tomou uma forma inerentemente paternalista, na medida em que requer uma suposição da vontade do titular dos direitos que não foi expressamente articulada.

No entanto, dado o grau em que as próprias empresas que captam dados demonstram que as pessoas ignoram os termos e condições que elas voluntariamente assinam, parece que impor algumas dessas obrigações aos serviços para proteger os dados de usuários individuais é proporcional e necessário[15]. E, claro que a privacidade, ela própria um direito fundamental, é um valor que o direito à segurança de dados e informações busca proteger (Soprana, 2018).

Existem diferentes formulações sobre o que o direito à privacidade acarreta, abrangendo desde a ideia bastante limitada de privacidade apenas ligada àquelas questões íntimas às quais uma expectativa razoável de privacidade pode se vincular a uma noção mais ampla de ao direito mais extremo de privacidade, para uma ideia ainda mais ampla, mais recente, de que o direito à privacidade está intimamente relacionado à proteção da identidade de alguém, a proteção e segurança de dados claramente se encaixa mais perto desta terceira denominação (Bioni, 2019).

Enquanto alguns dados como informações médicas podem ser do tipo que uma expectativa razoável de privacidade atribui, outros dados como por exemplo, dados de identificação, como endereço e número de telefone estão fora de esse escopo (Bioni, 2019).

E observando os apontamentos de Denardis (2014), a ideia do direito de ser deixado em paz pressupõe alguma intrusão na vida cotidiana, mas os vazamentos de Snowden

[15] *Relatório sobre a existência de um sistema global de intercepção de comunicações privadas e econômicas* (sistema de intercepção "ECHELON"). (2011). Estrasburgo: Parlamento Europeu. Recuperado em 09 de junho de 2019, de http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//PT.

mostraram que uma grande quantidade de vigilância acontece em segundo plano[16], sem o conhecimento daqueles cujos dados estão sendo coletados para esses fins.

Para Tene & Polonetsky (2013), contexto contemporâneo de práticas de vigilância onipresentes e o foco crescente na coleta e processamento de *Big Data*[17] impõe alguns desafios únicos ao direito à proteção de dados. Devido aos avanços da tecnologia, não há virtualmente nenhum limite para a quantidade de informação que pode ser registrada, não há virtualmente nenhum limite para o escopo da análise que pode ser feita, limitada apenas pela engenhosidade humana, e as informações podem ser armazenadas virtualmente para sempre.

O novo fenômeno que floresce é aquele no qual os dados recolhidos através das práticas de vigilância do cidadão comum que encontram o seu caminho, para os mecanismos de vigilância do Estado, através das empresas que detêm esses dados (Tene & Polonetsky, 2013).O próprio termo "*Big Data*" é um conceito notoriamente difícil de encontrar uma definição comumente aceita, mas uma série de recursos chave do *Big Data* foram identificados, incluindo o grande volume de dados, a velocidade com que são coletados, a variedade de dados, sua natureza relacional, permitindo que as ligações sejam feitas a outros conjuntos de dados (Tene & Polonetsky, 2013).

Costumava-se definir *'Big Data'* como sendo conjuntos de dados tão grandes que um supercomputador seria necessário para processá-los, outro aspecto do *'Big Data'* é que não apenas a capacidade analítica aumentou, mas também se tornou muito mais barata e amplamente distribuída (Viellechner, 2019). Não somente os dispositivos móveis de hoje têm mais poder de computação do que as máquinas *desktop* de uma década atrás, mas também que agora pode-se vincular dados e computadores virtualmente para que grandes tarefas computacionais possam ser realizadas de maneira acessível e conveniente.

O desafio para proteger o direito à proteção e segurança de dados hoje é a onipresença de dados voluntários, particularmente por meio do aumento de dispositivos vestíveis e redes de mídia social, embora os usuários de tais dispositivos possam não pensar em si mesmos como dados voluntários para outros como aponta as pesquisas de Pereira (2019).

---

[16] Bessa, J. (2014). *O escândalo da espionagem no Brasil*. Brasília: Thesaurus.

[17] *Big data* é definida pelo Lexico Oxford Dictionary como um conjunto de dados extremamente grandes que podem ser analisados computacionalmente de modo a revelar padrões, tendências e associações, especialmente relacionadas com o comportamento e interações humanas. Recuperado em 11 de julho de 2019, de https://www.lexico.com/en/definition/big_data.

O aumento da utilização de aplicativos de todas as variedades ou o auto rastreamento de informações biológicas, ambientais, físicas ou comportamentais por meio de dispositivos de rastreamento, dispositivos de Internet, informações de redes sociais e outros meios podem resultar na coleta de informações não apenas sobre o usuário individual, mas também sobre as pessoas ao seu redor (Castro, 2005).

Assim, como apontado por Mendonça (2018) um modelo exclusivamente baseado no consentimento não garante inteiramente a proteção dos dados de alguém, especialmente quando os dados coletados para uma finalidade podem ser reutilizados para outra.

Conforme revelado pelos vazamentos de Edward Snowden[18], a vigilância em massa é vista como um meio de prevenir crimes futuros, como ataques terroristas e ciberataques, e os observadores são menos visíveis do que no passado, dado que grande parte de sua vigilância é feita por meio de vigilância de dados, ou vigilância *online* e de dados de comunicações, em vez de movimentos físicos (Denardis, 2014).

Atualmente a luta da teoria dos direitos enfrentará dificuldades sobre os interesses que busca identificar e qualificar como direitos e os termos em que os enquadraria nas garantias constitucionais. Essas discordâncias serão, por sua vez, veículos para controvérsias sobre o equilíbrio adequado a ser alcançado entre alguns interesses individuais e algumas considerações sociais compensatórias, e será o principal gerador de inseguranças jurídicas pelo mundo (Pereira, 2019).

O equilíbrio correto a ser alcançado entre os interesses protegidos pelo direito à proteção de dados, conforme descrito acima, e se a redução de alguns aspectos desse direito constitui uma medida necessária e proporcional para a proteção da segurança nacional, este tema continuará a ser um assunto de debate para muitos anos vindouros (Rodotá, 2008).

Além disso, observando o trabalho de Guidi (2018) o direito à proteção de dados entra em conflito com o interesse da cooperação internacional em questões de segurança e, de forma mais geral, com o desejo das empresas de permitir a transferência gratuita de dados de suas operações em um país para uma de suas operações em um terceiro país.

Do ponto de vista das ciências jurídicas, há razões para acreditar que as atividades de vigilância serão ainda mais intensificadas e a cautela deve ser ecoada em todo o mundo sobre a tendência crescente de uso de algoritmos para prever tendencias sociais com fins de

[18] Bessa, J. (2014). *O escândalo da espionagem no Brasil.* Brasília: Thesaurus.

controles de massa dentro de todos os tipos de regimes, sejam eles totalitários ou democráticos (Pereira, 2019).

Essa forma de controle social tem o perigo inerente de perpetuar a discriminação e as suposições sobre certos grupos populacionais. A precisão desses métodos de originados do tratamento de informações dados não protegidos buscar prever com precisão os eventos futuros em potencial que podem ser questionados dentro da ordem social vigente (Rodotá, 2008). Aponta-se uma série de exemplos, incluindo as tentativas e o uso de análises para prever ou manipular os resultados de eleições nos EUA e em diversas democracias em redor do globo (Pereira, 2019). Esta tendência corre o risco de limitar os direitos humanos e as liberdades dos indivíduos, na medida em que as pessoas se autorregulam, tendo consciência de um estado de visibilidade cônscia e permanente, no sentido levantado por Foucault[19].

Além disso, o uso de dados e informações sensíveis como uma ferramenta de criação de perfil de civis pode ter o impacto de criar os próprios cenários que o regulador ou coletor de dados busca prevenir, ao transformar um cidadão inocente em um suspeito de terrorismo por meio da comparação e interpretação de peças de seus dados; visto que as informações e os dados, nesse sentido, tornam-se performativos, como já em testes em sistemas de inteligência no Reino Unido e na China (Elola, 2018).

O contexto contemporâneo de vigilância aprimorada tanto pelo estado quanto pelos cidadãos, o reaproveitamento de dados, a globalização e a cooperação internacional no processamento e coleta de informações e arquivos de dados, e o aumento do uso de algoritmos para prever riscos futuros, sem dúvida, apresentam desafios para a realização do direito à segurança e proteção de dados e informações (Elias, 2017).

Em uma ordem jurídica global em mudança, há uma necessidade maior do que nunca de refletir sobre a importância dos princípios que sustentam os direitos individuais e fundamentais em nossa sociedade, e em especial no âmbito do direito constitucional conforme sustenta Rodotá (2008). A Lei Internacional de Privacidade de Dados existe, em grande parte, para ajudar a facilitar um debate multinacional, bem informado e criterioso sobre os princípios que sustentam as respostas da sociedade a esses e outros desafios de segurança e proteção de dados. Embora as leis de maior alcance ainda sejam predominantemente europeias, a prontidão para estabelecer pelo menos equivalentes regulatórios rudimentares cada vez mais necessários ao redor do mundo.

[19] Foucault, M. (1987). *Vigiar e Punir: história da violência nas prisões*. Petrópolis: Editora Vozes.

3. A JUSTIÇA E O CONSTITUCIONALISMO DA PROTEÇÃO DE DADOS

A tecnologia da informação e comunicação em rápido desenvolvimento está transformando radicalmente nossa vida social e profissional. Cada vez mais nos comunicamos e interagimos com outras pessoas por meio de aplicativos eletrônicos de *smartphones, tablets, laptops* e mídias sociais *online* como observa Monteiro (2019).

Recentes violações de dados de alto nível e outras preocupações sobre como terceiros que protegem a privacidade de indivíduos na era digital levantaram inquietações nacionalistas sobre a proteção legal de dados eletrônicos em todo o mundo (Guidi, 2018).

As redes de computadores privadas e governamentais estão envoltas em práticas inadequadas de privacidade corporativa e segurança cibernética que expuseram informações pessoais de milhões de cidadãos em diversos países a destinatários indesejados (Dance, Confessore, & Laforgia, 2018). Ao mesmo tempo, a conectividade com a Internet aumentou e variou em suas diversas formas nos últimos anos.

Os membros de todas as classes sociais agora transmitem seus dados pessoais na Internet a uma taxa exponencialmente mais alta do que no passado, e seus dados são coletados, cultivados e mantidos por um número crescente de *players*, voltados para o consumidor, e, nos bastidores, como corretores e moderadores de dados conforme observamos o pensamento de Guidi (2018). Como consequência, a privacidade, a cibersegurança e a proteção de dados pessoais surgiram como uma questão importante para consideração do direito constitucional em diversos ordenamentos jurídicos mundo a fora que buscam sua inserção em suas respetivas legislações, ou a atualização de pontos que versarão sobres tais questões.

Além disso, muitos de nós estamos conectados quase permanentemente à rede mundial de computadores, acessando e recebendo informações e serviços por meio de tecnologia de comunicação móvel em tempo real (Dance, Confessore, & Laforgia, 2018).

A senda da pesquisa da lavra de Pereira (2018), observa que os dados deixados para trás são uma benção para as agências de aplicação da lei, mas também pode levar a uma interferência abusiva na vida privada de todos os cidadãos. As leis e políticas que acessam os dados de comunicação devem, portanto, equilibrar os benefícios da segurança com o respeito pelos direitos e garantias fundamentais e constitucionais.

Mede-se os padrões de privacidade e proteção de informações e dados sensíveis que Guidi (2018) observou tira-se lições para futuros esquemas de retenção de dados e outras políticas relacionadas a informações, arquivos e segurança de dados em nível global.

Embora algumas preocupações com a proteção de dados e de informações que derivem de como os governos pode utilizar esses dados, preocupações crescentes têm se concentrado em como o setor privado controla as informações digitais que coletam a todo segundo e armazenam em seus servidores (Lima, 2014). Práticas inadequadas de privacidade corporativa e invasões intencionais em redes privadas de computadores expuseram as informações pessoais de milhões de pessoas, que viram seus dados privados violados.

Ao mesmo tempo, a conectividade com a Internet aumentou de várias formas nos últimos anos, expandindo-se de computadores pessoais e telefones celulares a objetos do dia-a-dia, como eletrodomésticos, alto-falantes "inteligentes", veículos e outros dispositivos conectados de maneira ininterrupta à Internet (Elias, 2017).

Os Estados Unidos da América, como observa as pesquisas desenvolvidas por Elias (2017) agora transmitem seus dados pessoais na Internet a uma taxa exponencial, e junto com o aumento da conectividade, um número crescente de atores voltados para o consumidor como multinacionais, corporações, *sites* e, nos bastidores, como corretores e moderadores de dados além de empresas de publicidade coletam, mantêm e usam as informações dos consumidores sem o devido consentimento ou mesmo conhecimento de seus donos.

Embora essa coleta de dados possa beneficiar os consumidores norte-americanos por exemplo, permitindo que as empresas lhes ofereçam produtos mais personalizados, ela também levanta questões de privacidade, já que os consumidores muitas vezes não conseguem controlar como essas entidades usam seus dados. Como consequência, a proteção de dados pessoais surgiu como uma questão importante para consideração do mundo jurídico (Guidi, 2018).

Apesar do crescente interesse na proteção de dados, os paradigmas jurídicos que regem a segurança e a privacidade dos dados e informações sensíveis são complexos e técnicos como aponta Quelle (2017), e carecem de uniformidade a nível de um estado nacional para outro, ou mesmo em diferentes interpretações de tais paradigmais em seu ordenamento jurídico interno.

A Suprema Corte Americana por exemplo, reconheceu que a Constituição fornece vários direitos de proteção da privacidade individual, mas esses direitos geralmente protegem apenas contra intrusões do governo e fazem pouco para evitar que atores privados

abusem de dados pessoais *online*[20] nos termos da *4ª Emenda Constitucional das Proteções Constitucionais e o Direito à Privacidade*. No nível estatutário federal, embora haja uma série de estatutos de proteção de dados, eles regulam principalmente certas indústrias e subcategorias de dados (Elias, 2018).

A *Federal Trade Commission* dos EUA por sua vez preenche algumas das lacunas estatutárias ao aplicar a proibição federal contra práticas injustas e enganosas de proteção de dados [21]. Mas dentro do âmbito jurídico dos Estados Unidos da América, é possível constatar como aponta Elias (2017) que nenhuma lei federal única regula de forma abrangente e dinâmica a coleta e o uso de dados pessoais.

Em contraste com a natureza de colcha de retalhos da lei federal dos EUA, alguns governos estaduais e estrangeiros promulgaram uma legislação de proteção de dados mais abrangente[22]. Alguns analistas sugerem que essas leis, que incluem o RGPD da UE[23] e leis

[20] 4th amendment Constitutional Protections and the Right to Privacy of the U.S.A.

[21] 15 USC §§ 41-58 Federal Trade Commission Act; A Quarta Emenda da Constituição dos EUA estabelece que "o direito do povo de estar seguro em suas pessoas, casas, papéis e pertences, contra buscas e apreensões injustificadas , não deve ser violado e nenhum mandado deve ser emitido, mas por causa provável , apoiado por juramento ou afirmação, e particularmente descrevendo o local a ser revistado e as pessoas ou coisas a serem apreendidas . " O objetivo final desta disposição é proteger o direito das pessoas à privacidade e à liberdade de intrusões irracionais por parte do governo. No entanto, a Quarta Emenda não garante proteção contra todas as buscas e apreensões, mas apenas aquelas feitas pelo governo e consideradas injustificadas pela lei; Para alegar a violação da Quarta Emenda como base para suprimir uma evidência relevante, o tribunal há muito exigia que o reclamante provasse que ele próprio foi vítima de uma invasão de privacidade para ter legitimidade para reivindicar proteção sob a Quarta Emenda. No entanto, o Supremo Tribunal se afastou de tal exigência, a questão da exclusão deve ser determinada exclusivamente em uma resolução da questão substantiva se os direitos da Quarta Emenda do requerente foram violados, o que por sua vez exige que o requerente demonstre uma expectativa justificável de privacidade , que foi arbitrariamente violado pelo governo; Em geral, a maioria das buscas sem justificativa em instalações privadas são proibidas pela Quarta Emenda, a menos que uma exceção específica se aplique. Por exemplo, uma revista sem mandado pode ser legal, se um oficial pediu e obteve consentimento para fazer a busca; se a busca incidir sobre uma prisão legal; se houver causa provável para a busca e se houver circunstância exigente para a busca sem justificativa. Circunstâncias estranhas existem em situações em que as pessoas estão em perigo iminente, onde as evidências enfrentam destruição iminente ou antes da fuga iminente de um suspeito.

[22] Zachary SH. (2018). *A Litigator's Primer on European Union and American Privacy Laws and Regulations*.

[23] *Regulamento - UE 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Sobre a proteção de Pessoas Físicas no que diz respeito ao Processamento de Dados Pessoais e à Livre Circulação de Dados, e Revogação da Diretiva 95/46/ CE. Regulamento Geral de Proteção de Dados - RGPD.

estaduais, como o *California Consumer Privacy Act* (CCPA)[24], criarão regimes de proteção de dados cada vez mais sobrepostos e desiguais.

Este panorama jurídico fragmentado, juntamente com as preocupações de que as leis federais ou a níveis de toda uma nação existentes são inadequadas, levou muitas partes interessadas a argumentar que os governos de diversas democracias deveriam assumir um papel mais amplo na política de proteção de dados (Rodotá, 2008).

No entanto, no momento, não há consenso sobre o que, se houver, papel que o governo de uma nação deve desempenhar e quaisquer esforços legislativos de proteção e segurança de dados provavelmente implicarão em questões jurídicas únicas, como a regulação, legitimidade e direitos constitucionais relativos à segurança da informação pertencentes a civis, e até mesmo informações institucionais da administração pública, entre outras questões seguindo a senda da pesquisa de Guidi (2018).

3.1 Os desafios históricos relacionados ao constitucionalismo da proteção de dados

Quando diferentes direitos, como o direito à proteção de dados, o direito à liberdade de expressão e o direito à privacidade estão em jogo, os tribunais devem realizar um exercício de equilíbrio para reconciliá-los (Santos, 2018).

O direito à proteção de informações e dados como aponta Santos (2018) frequentemente interage com outros direitos, como a liberdade de expressão e o direito de receber e transmitir informações, contudo algo que muitos pesquisadores e legisladores perceberam com o tempo é que muitos desses pontos de interação então dentro da esfera constitucionalista do direito.

Esta interação é frequentemente ambivalente, embora existam situações em que o direito à proteção de dados pessoais está em conflito com um direito específico, há também situações em que o direito à proteção de dados e informações pessoais garante efetivamente o respeito desse mesmo direito específico. A necessidade de proteger os direitos e liberdades de terceiros é um dos critérios utilizados para avaliar a limitação legal do direito à proteção e segurança de dados pessoais (Rodotá, 2008).

[24] Cal. Legis. Serv. Ch. 55. CAL. CIV. (2018). CODE §§ 1798.100—1798.198.

O direito à proteção de dados pessoais é relativamente recente. O primeiro ato legislativo de proteção de dados foi promulgado em 1970 pelo estado alemão de Hesse[25], seguido pela Suécia em 1973[26] e, subsequentemente, por outros países europeus. Um dos primeiros exemplos de reconhecimento do direito à proteção de dados no nível constitucional é o Artigo 18[27] da Constituição Espanhola de 1978.

Embora o direito à proteção de dados não faça parte da Constituição dos Estados Unidos da América, nem da jurisprudência constitucional dos EUA, ele foi reconhecido pelas constituições de outros países que não os EUA desde os anos 70, e hoje é um direito fundamental na União Europeia, pois o direito à proteção de dados está consagrado no direito primário da União Europeia pela Resolução 679 de 2016, a denominada General Data Protection Regulation (GDPR, 2016)[28] ou Regulamento Geral de Proteção de Dados (RGPD, 2016) e nas constituições de vários países, a exemplo dos Estados Unidos, em que não há uma regulamentação para a proteção de dados válida de maneira uniforme para todo país, não obstante, o estado da Califórnia colocou em vigor no início de 2020 o California Consumer Privacy Act of 2018 (CCPA, 2018)[29], o Canadá possui, desde 2000, uma legislação nacional, a Personal Information Protection and Electronic Documents Act

---

[25] Datenschutzgesetz, 7 de outubro de 1970, §6, 1 Gesetz - und Verordnungsblatt für das Land Hessen. 1970.

[26] Datalagen (Swedish Data Act) de 11 de maio de 1973, entrou em vigor em 1º de julho de 1973.

[27] CJEU, processos apensos C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert v. Land Hessen, 9 de novembro de 2010.

[28] 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); Recuperado em 02 de julho de 2019, de https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-pt/format-PDFA1A#:~:text=Rate%20this%20publication-,Regulamento%20(UE)%202016%2F679%20do%20Parlamento%20Europeu%20e%20do,de%20Dados)%20(Texto%20relevante%20para.

[29] CÓDIGO CIVIL - CIV; DIVISÃO 3. OBRIGAÇÕES [1427-3273,16] (Título da Divisão 3 alterado pelas Estatísticas. 1988, Cap. 160, Seção 14.); PARTE 4. OBRIGAÇÕES DECORRENTES DE OPERAÇÕES PARTICULARES [1738-3273,16] (Parte 4 promulgada em 1872.); TÍTULO 1.81.5. California Consumer Privacy Act de 2018 [1798.100 - 1798.199.100] (Título 1.81.5 adicionado por Stats. 2018, Ch. 55, Sec. 3.); Recuperado em 11 de julho de 2019, de https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5..

(PIPEDA, 2000)[30], ou Lei de Proteção de Informações Pessoais e Documentos Eletrônicos e o Brasil seguindo o exemplo destes países criou a sua Lei Geral de Proteção de Dados[31] (LGPD, 2018).

O inicial reconhecimento constitucional do direito à proteção de informações e de dados considerados sensíveis, conforme observado pela cronologia jurídica histórica é provavelmente o Artigo 35 da Constituição de Portugal de 1976[32].

A Magna Carta Portuguesa de 1976 é possivelmente a primária constituição em toda a Europa a reconhecer o direito à proteção de informações e dados de seus cidadãos como uma garantia constitucional, onde em seu Artigo 35 versa que:

> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei. 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente. 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis. 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei. 5. É proibida a atribuição de um número nacional único aos cidadãos. 6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional. 7. Os dados pessoais constantes de ficheiros

[30] Lei de Proteção de Informações Pessoais e Documentos Eletrônicos; SC 2000, c. 5; Aprovado em 13/04/2000; Uma lei para apoiar e promover o comércio eletrônico protegendo as informações pessoais que são coletadas, usadas ou divulgadas em certas circunstâncias, fornecendo o uso de meios eletrônicos para comunicar ou registrar informações ou transações e alterando a Lei de Provas do Canadá, a Lei de Instrumentos Estatutários e a Lei de Revisão do Estatuto. Recuperado em 15 de setembro de 2019, de https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-1.html.

[31] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. 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. Recuperado em 01 de setembro de 2019, de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[32] A Constituição da República Portuguesa de 1976 é a atual constituição portuguesa. Foi redigida pela Assembleia Constituinte eleita na sequência das primeiras eleições gerais livres no país em 25 de Abril de 1975. Recuperado em 28 de junho de 2019, de https://www.parlamento.pt/parlamento/documents/crp1976.pdf.

> manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

Ainda no âmbito histórico, mas do direito espanhol, observamos na Constituição da Espanha de 1978, que consagra o direito à proteção de informações e dados no seu Artigo 18.4[33]. A conceituação do direito à proteção de dados na Espanha, em sua Constituição de 1978[34], está intimamente associada ao que se chamou de direito à autodeterminação da informação, oriundo da escola jurídica alemã, manifestada em dezembro de 1983 pelo Tribunal Constitucional da Alemanha[35].

Em 1992 a Espanha promulgou sua primeira lei de proteção de dados, a Lei Orgânica 5, de 29 de outubro de 1992[36], que regulamenta o processamento de dados pessoais por meios automatizados, e logo foi suprida pela lei que incorporou ao sistema jurídico espanhol a diretiva de proteção de dados de 1995. Desde 1993, o Tribunal Constitucional Espanhol assumiu a posição de que o direito à proteção de dados garantido pela Constituição espanhola é um direito fundamental separado e distinto do direito à privacidade[37].

---

[33] "A lei limitará o uso de sistemas informatizados para garantir o respeito pela honra e a vida privada da família dos cidadãos e o pleno exercício de todos os seus demais direitos." Artigo 18.4, Constituição da Espanha de 1978.

[34] A Constituição Espanhola de 1978 é a atual Constituição Espanhola; é a lei fundamental da organização jurídica espanhola, à qual ficam sujeitos os poderes públicos e os cidadãos da Espanha, em vigor desde 29 de agosto de 1978. Recuperado em 06 de agosto de 2019, de https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf..

[35] Em dezembro de 1983, o Tribunal Constitucional Federal Alemão declarou inconstitucionais certas disposições do Ato de Censo revisado (Volkszählungsurteil) que havia sido adotado por unanimidade pelo Parlamento Federal Alemão, quanto aos dados obtidos dos cidadãos; Rouvroy A., Poullet Y. (2009) The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. Recuperado em 22 de setembro de 2019, de https://doi.org/10.1007/978-1-4020-9498-9_2.

[36] Lei Orgânica nº 5, de 29 de outubro de 1992. Regulamenta o tratamento automatizado de dados pessoais. Recuperado em 18 de setembro de 2019, de http://legislacion.derecho.com/real-decreto-1720-2007-por-el-que-se-aprueba-el-reglamento-de-desarrollo-de-la-ley-organica-15-1999-de-13-de-diciembre-de-proteccion-de-datos-de-caracter.

[37] ACÓRDÃO 254/1993, de 20 de julho (BOE nº 197, de 18 de agosto de 1993); Tribunal Constitucional da Espanha; Recuperado em 03 de setembro de 2019, de http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383.

O conceito de direito à proteção de dados foi desenvolvido através de jurisprudência constitucional, consistente que o direito à segurança e proteção de dados não se restringe às informações privadas de um indivíduo, mas estende a proteção a todos os dados e informações pessoais, privados ou não, cujo conhecimento ou uso por terceiros possa afetar os direitos dos titulares dos dados, estejam esses direitos protegidos constitucionalmente ou não (Celeste, 2019).

Portanto, o âmbito do direito à proteção de dados não se limita ao direito à privacidade, que é protegido separadamente pelo Artigo 18, 1. da Constituição Espanhola e não pelo direito à proteção de dados. As informações não privadas seguindo a senda de Rodotá (2008) estão no âmbito do direito à segurança e proteção de dados, apesar de serem do conhecimento público.

Da mesma forma, o requisito de que os dados sejam pessoais não significa que apenas os dados relacionados com a vida privada das pessoas estejam sujeitos ao direito à proteção de dados, dando a este dispositivo um trato inteiramente constitucional e não como uma legislação complementar ou intermediaria, vindo a influenciar diretamente as redações futuras sobre as garantias jurídicas da proteção de dados (Celeste, 2019).

A jurisprudência e os regulamentos existentes demonstram que são de uma certa maneira inadequados para evitar os riscos e questões potenciais relacionados a esta mudança de paradigma na ordem social (Celeste, 2019). Isso se deve ao fato de que tanto o direito à privacidade quanto o direito mais recente, à proteção de dados e informações são protegidos como direitos individuais.

A dimensão social desses direitos, segundo Celeste (2019) tem sido levada em consideração por tribunais e legisladores em vários países como entendimentos constitucionais, mas este ainda é um movimento de vanguarda, visto a pluralidade de pensamentos dentro do âmbito jurídico do direito constitucional.

3.2 O constitucionalismo digital e suas responsabilidades

A governança de plataformas levanta preocupações constitucionais fundamentais no sentido de responsabilidades legais e sociais sobre como esses espaços sociais são constituídos e como o exercício do poder deve ser restringido, essas preocupações estão emergindo em um conjunto distinto de controvérsias em uma gama de plataformas diferentes

envolvendo diversos grupos de partes interessadas, incluindo usuários, empresas, governos e sociedade civil (Sunstein, 1996).

Desde então, as preocupações com a governança se multiplicaram e se intensificaram. Algumas das controvérsias mais visíveis giram em torno da privacidade e até que ponto os usuários consentem com o compartilhamento de dados detalhados sobre suas vidas e atividades com anunciantes e países (Gillespie, 2017).

Outros se concentram na visibilidade do conteúdo, à medida que as plataformas buscam classificar e ordenar as informações com base na relevância individual, em critérios que geralmente não são bem explicados e que às vezes parecem profundamente enviesados (Elias, 2017).

E, nos últimos tempos, conforme aponta os trabalhos de Gillespie (2017) aumentaram significativamente as solicitações para que as plataformas sejam mais responsáveis pela maneira como moderam a alocução, tanto de grupos que buscam maior responsabilidade das plataformas para lidar com o abuso quanto de grupos que buscam fortes restrições sobre a extensão em que as plataformas censuram a fala.

Conforme o mundo é consumido pelas novas tendencias digitais no meio social essas questões se estendem além das plataformas de comunicação para os mercados de *e-commerce* massivos e as plataformas de economia de pares emergentes que usam redes digitais para coordenar o fornecimento de bens e serviços em uma ampla gama da vida social (Elias, 2017). O papel das plataformas digitais como arquitetas de espaços públicos[38], sugere que elas deveriam ser mais responsáveis perante o público pelas formas como criam e aplicam as regras que regem nossas interações.

O estado de direito é um conceito bem estabelecido na teoria liberal ocidental que ancora a legitimidade da governança na legalidade. Logo o estado de direito exige que as decisões daqueles que têm poder sobre nós sejam tomadas de acordo com a lei, definida em oposição ao exercício arbitrário ou caprichoso do arbítrio humano (Rodotá, 2008).

Os valores do Estado de Direito, consentimento, previsibilidade e justiça processual são valores liberais fundamentais da boa governança (Black, 2012). Embora tenham sido historicamente limitados à esfera pública, argumento que esses valores fornecem um guia útil para a compreensão do papel que as plataformas online privadas desempenham no governo da vida social.

[38] Gillespie, T. (2017). *Governança de e por plataformas.* Burgess, J., Poell, T., Marwick, A. (Eds.), SAGE.

A estrutura do estado de direito fornece uma lente por meio da qual avaliar a legitimidade da governança *online* e, portanto, começar a articular quais limites as sociedades devem impor à autonomia das plataformas (Doneda, 2018).

Para que a governança de plataformas seja legítima de acordo com os valores do Estado de Direito, devemos esperar certas salvaguardas processuais básicas. Inicialmente, as decisões devem ser feitas de acordo com um conjunto de regras e não de uma forma arbitrária ou caprichosa (Rodotá, 2008).

Também é importante observar que essas regras devem ser claras, bem compreendidas e relativamente estáveis, e devem ser aplicadas de forma igual e consistente, devendo existir salvaguardas de devido processo adequadas, incluindo uma explicação do motivo pelo qual uma determinada decisão foi tomada e alguma forma de processo de apelação que permita a revisão independente e a resolução justa de disputas observando os pontos abordados pelo trabalho de Elias (2017).

Esses são os padrões mínimos de procedimentos fundamentais para que um sistema de governança seja legítimo, e as plataformas atualmente funcionam muito mal nessas medidas como observa (Doneda, 2018). Argumento que a extensão da influência que as principais plataformas e outros intermediários digitais têm sobre a vida social implica que devemos procurar responsabilizá-los por esses valores.

Isso não sugere a necessidade de qualquer mecanismo específico para garantir a legitimidade processual, e como aponta Gillespie (2017) não devemos esperar que as plataformas adotem os pesados padrões de uma democracia constitucional, por exemplo.

Em vez disso, responsabilizar as plataformas por esses valores sugere a necessidade de um processo contínuo de monitoramento, justificativa e melhoria dos sistemas que as plataformas implementam para regular o comportamento de seus usuários (Banisar, Guillemin, & Blanco, 2017).

Os conceitos vinculados de direitos dos usuários e responsabilidades das plataformas fornecem uma maneira útil de tornar explícitas as preocupações sobre a constituição de nossos espaços sociais *online* compartilhados (Gillespie, 2017).

Os valores do estado de direito fornecem a linguagem necessária para expressar essas preocupações e fazer avançar o projeto de constitucionalismo digital que busca articular e concretizar os padrões adequados de legitimidade para a governança na era digital (Elias, 2017).

Iniciando então, uma análise mais profunda entre os principais regulamentos e legislações pertinentes a este tema que se ramifica em diversos aspectos, será exposto e analisado suas devidas características, dividindo esta análise entre continente, iniciando-se pelo Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), atualmente em vigor na União Europeia que tem se destacado dentre diversos países e tem se firmado como um norte para diversas nações sobre legislações que versam sobre a segurança e proteção de dados, informações e boa governança das práticas estabelecidas nas novas rotinas sociais que estão se desenvolvendo e evoluindo rapidamente em compasso com as novas tecnologias desenvolvidas diariamente como aponta as recentes pesquisas apresentadas por Doneda (2018).

3.3 O modelo europeu de proteção de dados

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), em vigor na União Europeia busca enfrentar os desafios atuais relacionados à proteção de dados pessoais e harmonizar a proteção de dados em toda congregação de países que compõe a União Europeia. Embora almeja-se segundo Guidi (2018) que o RGPD (2016) beneficie as empresas, oferecendo consistência nas atividades e responsabilidades de proteção de dados nos países da União Europeia e permitindo políticas mais integradas de proteção de dados em toda a União Europeia.

Através das principais implicações práticas das mudanças foram identificadas e classificados aspectos que abrangem estratégias e práticas do Regulamento Geral sobre a Proteção de Dados, em que haverá uma obrigação legal dos estados conduzirem uma Avaliação de Impacto na Proteção de Dados pela primeira vez (Monteiro, 2019).

Logo, novas disposições e maneiras de sua implementação bem-sucedida mostra processos que operacionalizam os requisitos estabelecidos, garantindo a devida atenção aos direitos fundamentais, conforme Monteiro (2018) afiançados pelo RGPD, incorporando os novos requisitos desta importante legislação.

O Regulamento Geral de Proteção de Dados da União Europeia[39]é o desenvolvimento regulatório de maior consequência na política de informações em uma

[39] 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 de Proteção de Dados), JO 2016 L 119/1;

geração. O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) traz os dados pessoais para um regime regulatório complexo e protetor, visto que leis como o RGPD da União Europeia diferem em sua construção da maioria dos textos regulamentares, pois o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) pode ser visto como uma estrutura de governança de dados (Guidi, 2018).

O processo de conformidade do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) tenta colocar a proteção de dados e informações sensíveis e a privacidade no mesmo nível das leis que as empresas levam a sério, como leis antitruste e de práticas corruptas estrangeiras observando as pesquisas de Doneda (2019). Os mecanismos de aplicação do Regulamento Geral sobre a Proteção de Dados, apresenta determinações de penalidades, notificação ampliada de incidentes de segurança e requisitos processuais que têm o efeito de documentar desvios da lei impedirão de que as violações de privacidade sejam vistas como banalidades, além disso, a visão ampliada do Regulamento Geral sobre a Proteção de Dados sobre o que constitui uma "*violação*" significa que as empresas enviarão muito mais notificações de incidentes de segurança[40].

Desde a adoção do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) a privacidade e os dados pessoais estão sendo discutidos nos níveis mais altos das empresas e governos, pois a Europa há muito reconhece a privacidade explicitamente como um direito humano e os compromissos europeus vão além do lar, o foco de tantas leis busca de maneira eficaz e dentro do espaço do ordenamento jurídico constitucional, incluir proteções para a segurança da vida familiar, comunicações, reputação e, com o aumento da era da informação, para a privacidade no contexto do processamento de dados[41].

Recuperado em 16 de outubro de 2019, de http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[40] Relatórios de violações de dados ao Information Commissioner's Office do Reino Unido quadruplicaram nos meses em que o GDPR se tornou aplicável. M Schwartz, 'Under GDPR, Data Breach Reports in UK Have Quadrupled,' Bank Info Security; Recuperado em 13 de novembro de 2019, de https://www.bankinfosecurity.com/under-gdpr-data-breach-reports-in-uk-have-quadrupled-a-11249.

[41] O Artigo 8 da Convenção Europeia sobre Direitos Humanos de 1950, fornece proteção à vida privada e familiar, ao lar e às comunicações. Convenção para a Proteção dos Direitos Humanos e Liberdades Fundamentais, Artigo 8, 4 de novembro de 1950, 213 UNTS 222. A maioria das constituições nacionais na Europa também protegem a privacidade e os direitos relacionados. Observa-se a proteção constitucional da privacidade em países europeus: B.J. Koops, B. Newell, T. Timan, I. Škorvánek, T. Chokrevski, M. Galič, 'A Typology of Privacy,' (2017) 38 (2) University of Pennsylvania Journal of International Law 483.

3.3.1 Regulamento Geral de Proteção de Dados e os fundamentos da segurança da informação para sua regulação pública

Após anos de deliberações, em maio de 2016, o Parlamento Europeu e o Conselho de Ministros chegaram a um acordo sobre o texto final do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), que entrou em vigor diretamente nos Estados-Membros da União Europeia na primavera de 2018 (Foxx, 2018).

Representa uma modernização das regras de proteção de dados da União Europeia, substituindo a Diretiva de Proteção de Dados (DPD)[42] de 1995. O Regulamento Geral sobre a Proteção de Dados é geralmente considerado expansivo em termos de direitos de dados sujeitos as pessoas físicas identificadas ou identificáveis a quem as informações pessoais se relacionam e, em termos das obrigações e penalidades impostas aos controladores de dados, ou seja, aqueles que controlam o processamento de dados pessoais com o processamento definido de maneira ampla para incluir qualquer operação nos dados e informações pessoais, desde a coleta inicial por qualquer meio até a destruição final (Guidi, 2018).

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) confere às autoridades de proteção de dados poderes mais fortes, incluindo o poder de aplicar penalidades substanciais àqueles que violarem os direitos dos titulares de dados; em certos casos, até o valor de 20 milhões de euros ou 4% do faturamento global, o que for maior (Guidi, 2018). Diante de possíveis penalidades dessa magnitude, pode haver certa relutância em adotar tecnologias que tenham a complexidade do aprendizado de mecanismo de regulação do estado com dados e informações sensíveis e pessoais.

De acordo com o Regulamento Geral sobre a Proteção de Dados, um requisito essencial é que o processamento de dados pessoais seja baseado em um de vários motivos legais específicos, como o consentimento do titular dos dados de processar para uma finalidade específica ou no qual o processamento é necessário para o controlador cumprir uma obrigação legal. Requisitos adicionais, que segundo Foxx (2018) podem existir para categorias especiais de dados pessoais, como dados que revelam origem racial ou étnica ou dados genéticos, etc.

---

[42] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Recuperado em 06 de dezembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EL.

O processamento também deve seguir vários princípios fundamentais, incluindo que os dados sejam coletados para finalidades especificadas, explícitas e legítimas e não sejam processados de maneira incompatível com o princípio de limitação de finalidades e que o processamento seja limitado ao necessário para os fins específicos especificados pelo princípio de minimização de dados dos controladores de dados (Foxx, 2018).

Todas as organizações, ainda seguindo o pensamento de Foxx (2018) desde pequenas até grandes, públicas ou privadas, devem estar cientes de todos os requisitos do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) e estar preparadas para cumpri-los em sua integralidade, e o primeiro passo para cumpri-lo é designar um responsável pela proteção de dados que criará um programa de proteção e segurança de dados e informações para atender aos requisitos do RGPD (2016). Uma vez compatível, é importante manter-se informado sobre as mudanças na lei e nos seus métodos de aplicação.

O próprio Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) contém 11 capítulos e 91 artigos. A seguir, são apresentados alguns dos capítulos e artigos que têm maior impacto potencial nas operações de segurança, e em especial em funções de regulação publica que seriam conferidas aos Artigos 17 e 18, que concedem aos titulares de dados mais controle sobre os dados pessoais que são processados automaticamente (Viellechner, 2019).

O resultado é que os titulares dos dados podem transferir seus dados pessoais entre os provedores de serviços com mais facilidade, também chamado de “direito à portabilidade” e podem direcionar um controlador para apagar seus dados pessoais em determinadas circunstâncias, também chamado de direito ao apagamento ou esquecimento; Os Artigos 23 e 30 que exigem que as empresas implementem medidas razoáveis de proteção de dados para proteger os dados pessoais e a privacidade dos consumidores contra perda ou exposição; também os Artigos 31 e 32 versam sobre as notificações de violação de dados desempenham um papel importante no texto do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) seguindo muitos pontos abordados na obra de Doneda (2019).

O Artigo 31 especifica os requisitos para violações de dados únicos: os controladores devem notificar as Autoridades de Supervisão sobre uma violação de dados pessoais dentro de 72 horas após o conhecimento da violação e devem fornecer detalhes específicos da violação, como sua natureza e o número aproximado de sujeitos de dados afetados.

O Artigo 32 do RGPD (2016) exige que os controladores de dados notifiquem os titulares de dados o mais rápido possível sobre violações quando elas violam seus direitos e liberdades em alto risco; Os Artigos 33 e 34 a que exigem que as empresas realizem

avaliações de impacto na proteção de dados para identificar riscos aos dados do consumidor e análises de conformidade com a proteção de dados para garantir que esses riscos sejam tratados; O Artigo 35 exigindo que certas empresas nomeiem responsáveis pela proteção de dados. Especificamente, qualquer empresa que processe dados que revelem dados genéticos, saúde, origem racial ou étnica, crenças religiosas, etc. de um sujeito deve designar um responsável pela proteção de dados; esses executivos servem para aconselhar as empresas sobre o cumprimento da regulamentação e atuam como um ponto de contato com as Autoridades de Supervisão conforme aponta Soprana (2018).

Algumas empresas podem estar sujeitas a esse aspecto do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) simplesmente porque coletam informações pessoais sobre seus funcionários como parte dos processos de recursos humanos; Os Artigos 36 e 37 descrevem a posição do oficial de proteção de dados e suas responsabilidades em garantir a conformidade com o RGPD, além de relatar às autoridades de supervisão e titulares de dados; O Artigo 45 estende os requisitos de proteção de dados às empresas internacionais que coletam ou processam dados pessoais dos cidadãos da União Europeia, sujeitando-os aos mesmos requisitos e penalidades que as empresas baseadas na União Europeia e o Artigo 79 descreve as penalidades pelo não cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), que pode atingir até 4% da receita anual global da empresa infratora, dependendo da natureza da violação (Bassini, 2019).

No aprendizado de mecanismo de regulação do estado, em que dados de conjuntos de informações existentes ou coletados em tempo real são usados para treinar o algoritmo, e como algumas técnicas e aplicativos de aprendizado de mecanismo de regulação do estado são mais adequados para conjuntos de dados grandes, deve-se prestar atenção para evitar o processamento desnecessário dados pessoais (Foxx, 2018).

A conformidade com o princípio de minimização de dados pode limitar a aplicação de tais técnicas e resultar em uma imagem mais neutra, e por consequência menos representativa dos titulares dos dados (Soprana, 2018).

Abordando agora o objetivo do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) é impor uma lei uniforme de segurança de dados a todos os membros da União Europeia, para que cada estado membro não precise mais escrever suas próprias leis de proteção e segurança de dados e as leis sejam consistentes em toda a União Europeia (Viellechner, 2019).

Além dos membros da União Europeia, é importante observar que qualquer empresa que comercialize bens ou serviços para residentes da União Europeia, independentemente de sua localização, está sujeita ao regulamento (Soprana, 2018). Como resultado, o RGPD (2016) terá um impacto global nos requisitos de proteção de dados.

3.3.2 A importância da manutenção e reconhecimento de dados para a sua devida regulação no processamento de dados pessoais

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) mantém uma abordagem da Diretiva anterior, fixando os princípios gerais a serem observados em qualquer contexto de processamento de dados pessoais, inclusive em pesquisas e para fins de arquivamento de interesse público, e usando o tipo de dados e informações pessoais, inclusive no processamento de arquivos pessoais, dados registrados como dados pessoais personalizados, entre outras modalidades de registros de dados ou arquivos (Soprana, 2018).

No entanto, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) acrescenta três novos princípios gerais de importância. Os principais princípios gerais permanecem os mesmos que os termos da diretiva anterior (Philipp, 2016).

De fato, de acordo com o Artigo 6 do RGPD (2016), os dados pessoais devem ser tratados de maneira legal, justa e transparente na relação com o titular dos dados, sendo relevante e limitado ao necessário em relação aos fins para os quais são processados; preciso e, quando necessário, atualizado; também devem ser tomadas todas as medidas razoáveis para garantir que dados pessoais imprecisos, tendo em conta as finalidades para as quais são processadas, sejam apagadas ou retificadas sem demora; Mantidos de forma a permitir a identificação de titulares de dados por um período não superior ao estritamente necessário para atender os objetivos para os quais os dados pessoais serão utilizados (Bioni, 2019).

Outro princípio, segundo Bioni (2019) de aplicação geral do RGPD (2016) apareceu distintamente dos estabelecidos no Artigo 6, a saber, os princípios de proteção de dados por concepção e fixados no Artigo 25. Este novo princípio comercializa a abordagem integrada adotada pela União Europeia para criar um sistema sustentável de proteção de dados através do uso precoce de tecnologias adaptadas para melhorar a privacidade no *design* das operações de processamento e ao longo do ciclo de vida dos dados,

A União Europeia definitivamente aproxima a lei e a tecnologia, dois elementos essenciais do sistema de proteção de dados que devem ser desenvolvidos em conjunto para permitir a conformidade legal em um mundo moderno como bem ressalta Bioni (2019).

De acordo ainda com Bioni (2019) com essa abordagem tecnojurídica, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) declara que, considerando o estado da tecnologia, o custo de implementação e a sua natureza, juntamente ao escopo, contexto e objetivos do processamento de dados, arquivos e informações, bem como os riscos de probabilidade e severidade variáveis de direitos e liberdades de pessoas singulares colocadas pelo processamento, o responsável pelo tratamento deve, tanto no momento da determinação dos meios de processamento quanto no próprio momento do processamento, implementar medidas técnicas e organizacionais adequadas, como a pseudonimização[43], concebidos para aplicar de forma eficaz princípios de proteção e segurança de dados, como a minimização de dados, e integrar as salvaguardas necessárias ao tratamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos dos titulares de dados.

Essa abordagem de proteção e segurança de dados e de informações é algo bem conhecido em contextos de pesquisa científica abordados por Francisco D., & Francisco, S. (2019), notadamente no contexto do pedido de uma metodologia de implementação, em que o solicitante deve demonstrar a robustez do sistema de proteção de dados a ser praticado no curso da pesquisa para ser outorgado.

Os aspectos técnicos são completados por medidas organizacionais que permitem que a segurança e proteção dos dados seja respeitada, por exemplo, observando o plano de gerenciamento de informações, arquivos, dados, políticas e instruções de diretivas ligadas a privacidade, etc. (Soprana, 2018).

No entanto, esse recurso por projeto é concluído pelo padrão. Com este último, o responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas sejam processados os dados pessoais necessários para cada finalidade específica do tratamento. Essa obrigação se aplica à

[43] Nos termos do número 5 do artigo 4.º do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679, entende-se por 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".

quantidade de dados pessoais coletados, à extensão de seu processamento, ao período de seu armazenamento e à sua acessibilidade (Soprana, 2018).

Em linha ao pensamento de Doneda (2018), essas medidas devem garantir que, por padrão, os dados pessoais não sejam acessíveis sem a intervenção do indivíduo a um número indefinido de pessoas singulares, buscando prezar pela ética do RGPD (2016) e evitar eventuais abusos.

Uma observação quanto ao RGPD (2016) são suas características como uma normal que estipula um padrão em serie de especificidade de que somente o sistema deve garantir proteção suficiente sem nenhuma ação humana. No entanto, não deve ser totalmente autônomo, pois criaria um risco em termos de controle de dados e, portanto, uma perda do recurso de proteção do critério por padrão (Rodotá, 2008).

Além desses princípios norteadores, Philipp (2016) faz observações importantes sobre o Artigo 9 do RGPD (2016) que fixa regras gerais sobre o respeito ao processamento de dados pessoais sensíveis, como dados sobre saúde ou dados genéticos, e mantém os mecanismos anteriores baseados em uma proibição geral de processamento, com algumas exceções importantes, em particular, para a prática da saúde e a gestão dos sistemas de saúde, saúde pública e pesquisar setores em que o processamento é autorizado sob condições específicas.

Com foco na proteção de dados, ainda de acordo com o Artigo 9, o processamento de dados pessoais sensíveis para fins de arquivamento de interesse público, para fins de proteção de dados científica ou histórica ou para fins estatísticos será necessário, para benefício das pessoas singulares e da sociedade, conforme necessário. um todo e com base no direito da União ou dos Estados-Membros, que seja proporcional ao objetivo prosseguido, respeite a essência do direito à proteção de dados e preveja medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados (Bioni, 2019).

Neste ponto, observa-se a nova importância de buscar um objetivo de interesse público para justificar o tratamento de informações e dados pessoais sensíveis, conforme explicado claramente nos Artigos 53 e 54. Além disso, disposições fundamentais, o RGPD (2016) também introduz novas definições importantes que fundamentarão uma interpretação mais aprofundada do RGPD (Philipp, 2016).

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) completa os princípios citados acima, fixando requisitos de aplicação geral relativamente novos no seu

Artigo 6, que existem sob a Diretiva anterior, mas que agora adquiriu uma nova dimensão (Monteiro, 2019).

O princípio elementar é sobre o respeito à integridade dos dados e à sua confidencialidade. Esse princípio impõe que os dados sejam processados de maneira a garantir a segurança adequada dos dados pessoais, incluindo a proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, usando medidas técnicas ou organizacionais apropriadas (Gurses, Troncoso, & Diaz, 2015).

Esse princípio aplica-se não apenas a aplicação de regras de profissionais de saúde e diretrizes de ética em pesquisa, como aquelas que garantem a integridade científica e de pesquisa, mas também o meio de medidas técnicas, como o uso de técnicas de codificação por exemplo, técnicas de pseudonimização, criptografia ou anonimização[44], uso de servidores protegidos contra ameaças externas, sistema de processamento de dados controlados por controle, etc. (Soprana, 2018).

Esse princípio é particularmente importante no contexto de pesquisa em que um grande potencial de dados confidenciais está em risco e no qual a qualidade dos dados é essencial para garantir que os resultados da pesquisa possam ser usados, verificáveis e úteis (Gurses, Troncoso, & Diaz, 2015).

O princípio acessório, que também existe sob a diretiva anterior, é o princípio da responsabilidade. De acordo com esse princípio, o responsável pelo tratamento deve ser responsável por evidenciar a capacidade de demonstrar a conformidade com os princípios gerais de processamento de dados expostos acima (Philipp, 2016).

Isso exige, em particular, um agente responsável pelo tratamento, ou, quando aplicável, seus representantes na União Europeia, e os registros organizados e que se mantenham claros e seguros de todas as atividades de processamento de dados executados sob sua responsabilidade, para os fins de demonstrar a eficiência e a boa execução do RGPD (Gurses, Troncoso, & Diaz, 2015).

Esses registros podem constituir arquivos retidos por um período de tempo determinado, de acordo com a lei aplicável. Ressaltando que Regulamento Geral sobre a

[44] A anonimização consiste em técnicas que dividem a informação, de modo a que não seja possível a identificação do titular dos dados, tratando-se de uma operação irreversível, diversamente, a pseudonimização consiste em técnicas de separação de dados de modo a impossibilitar a identificação do titular dos dados, contudo é possível agregar os dados de modo a que seja identificado o titular dos dados, utilizando-se em situações em que seja necessário identificar o titular dos dados.

Proteção de Dados (RGPD, 2016) detalha explicitamente como as informações mínimas devem ser preservadas nos registros de acordo com o Artigo 30, em que cada *driver* e processador deve ser obrigado a cooperar com a autoridade supervisora e disponibilizar esses registros, para aqueles que estabelecem a responsabilidade de monitorar essas operações de processamento, onde considera-se também os testes organizados e a busca pela conservação de registros claros e seguros de todas as atividades de processamento e de dados armazenados sob sua responsabilidade (Philipp, 2016).

A regulamentação corporativa, contudo, não está funcionando de forma a proteger nossos dados. Empresas e outras organizações ao redor do mundo que coletam dados de pessoas há muito tempo defendem a regulamentação da privacidade e da proteção de dados por meio de estruturas de autorregulação ou co-regulamentação que lhes oferecem maior flexibilidade como bem observou Gellert (2018). No entanto, apesar de várias tentativas, ainda não vimos exemplos desse tipo de regulamentação que sejam positivos para os direitos dos usuários ou para o negócio como um todo.

A conformidade destas regras do RGPD (2016) é de extrema importância, pois tais pontos buscam garantir o direito fundamental da segurança de dados e informações, além de acentuar a responsabilidade constitucional dos operadores públicos e privados no tratamento e segurança da informação e dos dados (Waldman, 2018).

3.3.3 As novas definições de tratamento de dados do Regulamento Geral sobre a Proteção de Dados

O entendimento da terminologia legal é fundamental para garantir sua adequada disseminação e aplicação pelas partes interessadas. No campo da proteção de dados, os atores jurídicos encontraram dificuldades em compreender e contornar noções que são cientificamente baseadas e dependentes da evolução de tecnologias e contextos sociológicos (Rodotá, 2008).

Com o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), pode-se saudar o trabalho realizado pelo legislador da União Europeia para elaborar várias definições de utilidade direta no contexto da pesquisa científica e que representam a nova referência comum para os Estados-Membros como afirma Philipp (2016).

Em particular, o RGPD (2016) introduz algumas novas definições de determinadas categorias especiais de dados pessoais cujo processamento é proibido, por princípio, mas excepcionalmente admitido para fins de pesquisa ou arquivo de interesse público, no que diz respeito aos Artigos 9 e 89.

Como por exemplo Dados relativos à saúde[45], dados pessoais relacionados à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre seu estado de saúde e quadro clinico geral, e pode-se constatar que essa noção é definida inclusive como todos os dados pertencentes ao *status* de saúde de um titular de dados que revelam informações relacionadas ao passado, estado de saúde física ou mental atual ou futura do titular dos dados (Aieta, 2014).

Isso inclui observando a obra de Castro (2005) informações sobre a pessoa singular coletada durante o registro ou a prestação de serviços de saúde, sendo abordando inclusive na Directiva 2011/24/UE[46] do Parlamento Europeu e do Conselho da União Europeia sobre os direitos de saúde transfronteiriços da pessoa natural. Um número, símbolo ou ícone particular poderia ser atribuído a uma pessoa singular para identificar exclusivamente a pessoa especifica para fins de saúde; Informações derivadas de testes ou exames de uma parte do corpo ou substância corporal, incluindo dados genéticos e amostras biológicas; e qualquer informação sobre, por exemplo, uma doença, incapacidade, risco de doença, histórico médico, tratamento clínico ou o estado fisiológico ou biomédico do titular dos dados independentemente de sua fonte, por exemplo, de um médico ou de outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*, estariam disponíveis, no entanto sob o manto das normas jurídicas de proteção e segurança de informações e dados (Philipp, 2016).

Dados genéticos[47], por exemplo que são também considerados dados pessoais e sensíveis, visto que estão relacionados com as características genéticas herdadas ou

---

[45] Artigo 4 (15) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679.

[46] Directiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de Março de 2011 , relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços. OJ L 88, 4.4.2011, p. 45–65. Recuperado em 27 de novembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0024&from=EN.

[47] Artigo 4 (13) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679. Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

adquiridas de uma pessoa singular, e que fornecem informações únicas sobre a fisiologia, etnia ou a saúde dessa pessoa especifica e que resultam, em particular, de uma análise de uma amostra biológica da pessoa em questão como observava Aieta (2014).

Além disso, o considerando informação especifica, em que os dados genéticos podem consistir em resultado da análise de uma amostra biológica da pessoa singular em questão, em particular análises cromossômicas, ácido desoxirribonucleico (DNA) ou ácido ribonucleico (RNA) ou da análise de outro elemento que permita informações equivalentes para ser obtido como observa Aieta (2014).

A última parte desta sessão pode desencadear questões relativas aos limites da noção de dados genéticos que devem ser restritivos em vez de extensos. Com essa abertura, é difícil entender que tipo de dados poderia ser qualificado como dados genéticos (Monteiro, 2019).

Essas informações como as genealógicas poderiam ser coletadas por meio de questionários? Isso poderia ter como objetivo dados epigenéticos? Até certo ponto, isso cria confusões com relação à noção de dados biométrico[48], dados pessoais resultantes de processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a identificação única dessa pessoa especifica, como imagens faciais ou dados dactiloscópicos. Seja como for, essa definição parece ser uma base muito útil e viável, porem um ponto sensível a ser observado nas cortes de justiça (Monteiro, 2019).

Com relação à condição dos dados, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) também adota novas definições, as de pseudonimização e criptografia, e confirma a noção anterior de dados anônimos (Soprana, 2018).

A Pseudonimização[49], o tratamento de dados pessoais de modo a que os dados pessoais já não possam ser atribuídos a um titular de dados específico sem a utilização de

[48] Artigo 4 (14) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679.

[49] Artigo 4 (5) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679 e considerando-se os artigos 26º dos Responsáveis conjuntos pelo tratamento; 1. Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13º e 14º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados; 2. O acordo a que se refere o nº 1 reflete devidamente as funções e relações respetivas dos responsáveis

informações adicionais, desde que essas informações adicionais sejam mantidas separadamente e sujeitas a procedimentos técnicos e organizacionais (Soprana, 2018). Medidas para garantir que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável.

O resultado da pseudonimização são dados *pseudonimizados* que permanecem dados pessoais, mas são protegidos por codificação ou criptografia. Em todo o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) o uso da pseudonimização é promovido e deve ser implementado, tanto quanto possível, no processamento de dados pessoais para fins de

---

conjuntos pelo tratamento em relação aos titulares dos dados. A essência do acordo é disponibilizada ao titular dos dados; 3. Independentemente dos termos do acordo a que se refere o nº 1, o titular dos dados pode exercer os direitos que lhe confere o presente regulamento em relação e cada um dos responsáveis pelo tratamento e 28º do Subcontratante; (3). O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante: a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público; b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade; c) Adota todas as medidas exigidas nos termos do artigo 32º; d) Respeita as condições a que se referem os nº 2 e 4 para contratar outro subcontratante; e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III; f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32º a 36º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante; g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

pesquisa científica, como uma prática padrão de proteção e segurança de informações e dados[50](Soprana, 2018).

Já os Dados anônimos[51] são definidos como informações que não se relacionam com uma pessoa física identificada ou identificável ou com dados pessoais tornados anônimos de tal maneira que o titular dos dados não é ou não é mais identificável (Rodotá, 2008).

O presente regulamento não diz respeito, portanto, ao tratamento de tais informações anônimas, inclusive para fins estatísticos ou de pesquisa (Soprana, 2018). Além disso, entre as questões relacionadas aos direitos dos titulares dos dados, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) fornece uma nova definição do termo de consentimento.

Existe também a previsão do consentimento previsto pelos dispositivos do RGPD (2016) do titular dos dados[52], que significa qualquer indicação dada livremente, específica, informada e inequívoca dos desejos do titular dos dados pelos quais ele, em uma declaração ou uma ação afirmativa clara, constituem concordância com o processamento de dados pessoais relacionados ao titular das informações (Gellert, 2018).

Aqui, observa-se que a noção de Gellert (2018) foi especificada em relação à característica inequívoca do consentimento, que não levanta dúvidas sobre o escopo das atividades acordadas pelos titulares dos dados e sobre a forma de consentimento que deve ser uma declaração ou uma afirmação clara de ação. As novas regras relativas ao consentimento do titular dos dados, inclusive no campo de pesquisa, estão expostas e devidamente catalogadas pelas normas impostas pelo RGPD (2016).

Alguns pontos são levantados quanto ao Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) não definir noções como "*cloud Computing"*[53] ou mesmo do "*Big*

---

[50] Recuperado em 11 de novembro de 2019, de https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt.

[51] Artigo 26 do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679.

[52] Artigo 4 (11) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679. Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

[53] Cloud Computing ou Computação em nuvem é um termo coloquial para a disponibilidade sob demanda de recursos do sistema de computador, especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador. Recuperado em 12 de dezembro de 2019, de https://aws.amazon.com/pt/what-is-cloud-computing/.

Data"[54], que são frequentemente usadas em debates sobre proteção de dados sem definição legal harmonizada, mas além desses avanços terminológicos, o RGPD inova na maneira como a proteção de dados será garantida na prática, estabelecendo alguns novos procedimentos a serem seguidos. Seja como for, essa definição parece ser uma base muito útil e viável em nossos tempos, de tecnologias que avançam em ritmo frenético e constante interagindo diariamente com a rotina e o modo como a sociedade se organiza. (Tene & Polonetsky, 2013).

A computação em "nuvem" está na moda, mas apesar do uso excessivo e impróprio do termo, está cada vez mais claro que muitos dos dados e recursos que costumávamos acreditar que devíamos possuir localmente em computadores, dispositivos portáteis, sistemas de entretenimento e negócios sistemas de registro, agora podem ser fornecidos com maior segurança e confiabilidade e a um custo menor remotamente (Tene & Polonetsky, 2013).

Na verdade, testemunha-se o movimento desse poder computacional, bem como o armazenamento da onda gigante de dados que estamos gerando e coletando, para a "nuvem" ou como "*cloud Computing"* como apontou Milakovich (2012).

3.3.4 Impacto jurídico pratico da Proteção de Dados

Quando é provável que um tipo de processamento resulte em alto risco para os direitos e liberdades dos titulares dos dados, os controladores de dados devem executar uma Avaliação de Impacto na Proteção de Dados (Gellert, 2018).

Uma Avaliação de Impacto na Proteção de Dados é necessária, particularmente nos casos de uma avaliação sistemática e abrangente de aspectos pessoais relacionados a pessoas físicas, com base no processamento automatizado, incluindo criação de perfis, visto o Artigo 35, 3, a, do RGPD (2016). De acordo com o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), a Avaliação de Impacto na Proteção de Dados deve abranger, entre outras coisas, as medidas de segurança destinadas a garantir a proteção de dados pessoais e a conformidade com o regulamento (Philipp, 2016).

[54] Big Data, segundo o Oxford Big Data Institute, é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados que são gerados atualmente para serem analisados por sistemas interdisciplinares. Recuperado em 07 de dezembro de 2019, de https://www.bdi.ox.ac.uk/.

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) refere-se, em particular, aos casos em que o processamento de dados pessoais dos titulares de informações para fins de criação de perfil que podem gerar ou causar discriminação com base em qualquer uma das categorias especiais de dados, por exemplo. origem racial ou étnica, religião, estado de saúde, etc. ou a medidas que tenham esse efeito discriminatório (Gellert, 2019).

Ainda segundo Gellert, 2018 (2018) ele impõe ao estado que regula e protege os dados a obrigação de usar procedimentos matemáticos e estatísticos adequados para a criação de um perfil social em rede, a fim de garantir que os fatores que resultam em imprecisões nos dados pessoais sejam corrigidos e o risco de erros seja minimizado.

A discriminação injusta em um ambiente de aprendizado de mecanismo de regulação do estado pode ser causada por um viés direto ou indireto introduzido no processo de criação de perfil devido a deficiências na qualidade e quantidade dos dados disponíveis para treinar e testar o algoritmo, bem como problemas com fontes de dados, sua averiguação, qualificação e rotulagem (Pereira, 2019).

Portanto, os legisladores e controladores de dados devem implementar medidas apropriadas para mitigar o risco de algoritmos trabalharem com dados incompletos ou não representativos, os quais podem gerar correlações espúrias que resultam em decisões injustificáveis conforme Mendes & Mattiuzzo (2019).

Mesmo que não sejam explicitamente mencionadas dentro da norma, as medidas de segurança mencionadas podem exigir que os controladores de dados implementem os princípios de proteção de dados por projeto e por padrão nos termos do Artigo 25 do RGPD, tanto no momento da determinação dos meios de processamento, por exemplo, ao decidir usar algoritmos de aprendizado de mecanismo de regulação do estado para processar dados pessoais e no momento do processamento em si (Proxxima, 2018).

Portanto, observando a obra de Mendes & Mattiuzzo (2019) em um contexto de aprendizado de mecanismo de regulação do estado, por exemplo, a fim de cumprir o princípio de minimização de dados discutido acima, os controladores de dados podem ter que decidir, no momento da coleta, quais dados pessoais serão processados para fins de criação de perfil.

Em seguida, eles também deverão fornecer ao algoritmo apenas os dados estritamente necessários para a finalidade específica de criação de perfil, mesmo que isso leve a uma representação mais restrita do titular dos dados e possivelmente a uma decisão menos justa para todos (Mendes & Mattiuzzo, 2019).

Novamente, os sistemas de aprendizado de mecanismo de regulação do estado podem ser compostos por uma natureza algorítmica artificial, tendo sido projetados por uma parte que não seja o legislador ou controlador de dados e com dados de entrada derivados de uma variedade de provedores de dados separados, e os processos de aprendizado de mecanismo de regulação do estado podem ser executados em um ambiente "*cloud Computing"* ou em "*nuvem"* que pode envolver vários provedores de serviço (Proxxima, 2018).

Portanto, conforme a abordagem de Guidi (2018) o controlador de dados pode ter dificuldades para implementar as medidas técnicas e organizacionais apropriadas exigidas pelo RGPD para cumprir os princípios de proteção de dados.

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) busca preservar o equilíbrio entre a necessidade de proteger efetivamente os direitos dos titulares de informações e dados em um mundo digitalizado e globalizado, permitindo o processamento de informações pessoais, incluindo dados confidenciais, para pesquisas científicas (Guidi, 2018).

Reforçando as obrigações de cooperação e a transparência entre os atores do processamento de informações, internamente e em relação às autoridades de supervisão, que devem criar um sistema de proteção de dados da União Europeia mais integrado e diminuir alguns custos administrativos inúteis, descentralizando elementos da governança da segurança e proteção de dados e informações em relação aos controladores de dados e processadores de dados (Proxxima, 2018).

É importante ressaltar que embora o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) adote e estimule novas disposições específicas para garantir a proteção de dados, adaptadas por exemplo nos mecanismos de busca ou de pesquisa, o campo permanece amplamente regulamentado no âmbito de países, em particular no que diz respeito ao tratamento e à aplicação dos direitos de segurança de informações e liberdade de expressão dos cidadãos, quanto a utilização destas ferramentas de pesquisa, onde os reguladores podem ser contrários a estes princípios ou inclinados a sua regulação de maneira mais rígida, devendo sempre os legisladores e o poder judiciário garantir e atribuírem a ética e os direitos fundamentais como princípios constitucionais balizadores na sua regulação. (Böckenförde, 2017).

Contudo, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) tem o mérito de estabelecer regras mais claras que servirão positivamente às práticas de pesquisa, especialmente quanto as regras estabelecidas para o consentimento, no que diz respeito às

regras para reutilizar dados pessoais para outro fim, avaliar os riscos do processamento de dados no contexto da Avaliação de Impacto na Proteção de Dados, adotando um sistema de gerenciamento responsável de processamento operações e construção ou reforço de competências internas de proteção de dados gera um ambiente seguro contra eventuais ameaças a segurança das informações públicas e privadas (Proxxima, 2018).

Além disso, pela primeira vez, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) se refere ao respeito aos padrões éticos como parte da legalidade do processamento da pesquisa, o que deve ser saudado como um esforço pela consistência específica do setor. Finalmente, o RGPD abre novas possibilidades para avançar na estruturação do compartilhamento de dados em pesquisas científicas com medidas que incentivam o desenvolvimento da auto regulação (Proxxima, 2018).

A legislação da União Europeia em matéria de proteção de dados pressupõe que os processos automatizados de tomada de decisões sejam arriscados e que os indivíduos precisam ser protegidos de tais processos. As proteções específicas incluem o direito de ser informado sobre a tomada de decisões automatizada, incluindo a criação de perfil, bem como o direito de uma revisão humana de uma decisão de mecanismo de regulação do estado (Guidi, 2018).

Com os avanços na pesquisa de aprendizado de mecanismo de regulação do estado ressaltando os apontamentos de Proxxima (2018), uma possibilidade interessante é que os mecanismos de regulação do estado superem certas limitações dos tomadores de decisão humanos e nos forneçam decisões que sejam comprovadamente justas e condizentes com nossas normativas jurídicas, valores constitucionais e convenções sociais.

3.4 O modelo do continente americano de proteção de dados

Antes de 2018, vários países latino-americanos já tinham algumas medidas de políticas de proteção de dados em vigor como observa Elola (2018). Após a entrada em efetiva do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) no âmbito da apreciação do ordenamento jurídico mundial, estamos testemunhando um surto de emendas a leis de privacidade, à medida que os países latino-americanos elevam seus padrões de proteção de dados para atender aos estipulados na regulamentação da União Europeia[55].

[55] Baker & McKenzie Global Privacy Handbook comparar uma série de tópicos e jurisdições dentro do domínio da privacidade e sobre capitação de dados. Baker McKenzie (2018); Global Privacy and Information

A União Europeia é tradicionalmente conhecida por definir o padrão para regulamentações de proteção de dados em todo o mundo e o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) não é exceção. Com base em suas disposições de proteção de dados de ponta e medidas e sanções rígidas, o RGPD já está impactando a legislação mundial e está definindo o mais alto padrão no tratamento de dados pessoais (Gellert, 2018).

Os Estados Unidos da América seguem o que é conhecido como abordagem 'setorial' da legislação de proteção de dados (Soprana, 2018). Sob essa abordagem, as leis de proteção de dados e privacidade dependem de uma combinação de legislação, regulamentação e autorregulação, e não apenas da interferência governamental[56].

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) alcançou relevância internacional, não apenas porque contém disposições amplas relacionadas à proteção de dados pessoais e privacidade, mas também devido à sua aplicação extraterritorial. O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) pode impor obrigações não apenas a empresas localizadas na União Europeia que processam dados pessoais, mas também a empresas localizadas em países fora da União Europeia que processam dados pessoais de cidadãos da União Europeia (Monteiro, 2019).

Este regulamento, recapitulando, também conferiu às autoridades da União Europeia o poder de conduzir as conclusões de adequação. As autoridades podem avaliar se um terceiro país, território ou setor de um terceiro ou de uma organização internacional garante um nível adequado de proteção de acordo com as disposições do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016). Os países fora da União Europeia podem ter uma motivação financeira para impor obrigações de proteção de dados no nível do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), a fim de colher os benefícios potenciais de ter suas disposições domésticas consideradas adequadas no âmbito do RGPD para transferências de dados da União Europeia (Gellert, 2018).

Management; Handbook; Recuperado em 28 de dezembro de 2019, de https://tmt.bakermckenzie.com/-/media/minisites/tmt/files/global_privacy_handbook-_2018.pdf?la=en.

[56] Solove, D. & Hartzog, W. (2014). *The FTC and the New Common Law of Privacy*, 114, Colum. L. Rev. 583, 587; "A lei estatutária é difusa e discordante ... Ao contrário das leis de privacidade de muitas nações industrializadas, que protegem todos os dados pessoais de forma omnibus, a lei de privacidade nos Estados Unidos é setorial , com diferentes leis que regulam diferentes indústrias e setores econômicos ... Esta abordagem setorial também deixa grandes áreas não regulamentadas ... ".

Observa-se como os principais polos de circulação de informações no hemisfério norte e no hemisfério sul do continente americano conforme Bioni (2019) vem posicionando-se ante as novas tendencias de dispositivos jurídicos de proteção de dados, com foco especial em sua paridade com o regulamento europeu, como veremos nos tópicos a seguir, analisando países do continente americano.

3.4.1 Os Estados Unidos da América

A Lei de Proteção de Dados trata da segurança da transmissão eletrônica de dados pessoais. Até o momento, os Estados Unidos da América não têm nenhuma legislação formal e centralizada em nível federal com relação a essa questão, aponta Elola (2018), mas garantem a privacidade e a proteção de dados por meio da Lei de Privacidade dos EUA, da Lei de Porto Seguro e da Portabilidade e Responsabilidade de Seguro Saúde.

Desde o governo de Bill Clinton, os Estados Unidos da América seguiram uma política voltada para permitir que o setor privado liderasse o caminho na proteção de dados. Isso significa que as empresas devem implementar suas próprias políticas, desenvolver sua própria tecnologia e os indivíduos devem se autorregular para evitar a disseminação de seus dados privados (Morais & Neto, 2014). De acordo com essa política, os EUA ainda não desenvolveram uma única lei federal de proteção de dados.

De acordo com a abordagem setorial dos Estados Unidos da América, entretanto, a legislação de privacidade tende a ser esparsa e apenas adotada em uma base "*ad hoc*"[57], com a legislação surgindo quando as circunstâncias exigirem, ressalta Elola (2018). Essas leis geralmente se aplicam apenas a situações nas quais os indivíduos não seriam capazes de controlar o uso de seus dados por meio de autorregulamentações. Os exemplos incluem a

[57] Ad hoc é uma expressão latina cuja tradução literal é "para isto" ou "para esta finalidade". É geralmente empregada sobretudo em contexto jurídico, também no sentido de "para um fim específico". Oxford Languages. Recuperado em 01 de março de 2019, de https://languages.oup.com/google-dictionary-pt/.

Lei de Proteção à Privacidade de Vídeo de 1988[58], a Lei de Proteção e Concorrência de Televisão a Cabo de 1992[59] e a Lei de Relatórios de Crédito Justo[60].

As tradições da lei de privacidade americana ainda segundo Elola (2018) girão em torno do raciocínio por trás da abordagem dos EUA em que às leis de privacidade tem tanto a ver com a economia americana quanto com sua tradição jurídica. Por exemplo, embora os Estados Unidos da América tenham valorizado tanto seu direito à liberdade de expressão que a primeira emenda à Constituição dos Estados Unidos da América o protege explicitamente, a Constituição não tem um direito explícito à privacidade.

A Suprema Corte dos Estados Unidos da América concluiu que o direito à privacidade está implícito nos termos de outras partes da Constituição, e muitos estados têm direitos explícitos à privacidade em suas constituições estaduais, mas em nível federal não há garantia constitucional expressa de privacidade, conforme observado pela obra de Guidi (2018).

---

[58] O Video Privacy Protection Act (VPPA) foi um projeto de lei aprovado pelo Congresso dos Estados Unidos em 1988 como Pub.L. 100-618. Esta lei foi criada para evitar o que se chama de divulgação indevida de registros de aluguel ou venda de fitas de vídeo ou materiais audiovisuais semelhantes, para cobrir itens como videogames e o futuro formato de DVD. Faz com que qualquer provedor de serviços de fita de vídeo que divulgue informações de aluguel fora do curso normal dos negócios seja responsável por até $ 2500 em multa por danos ao prejudicado pela ação. Recuperado em 12 de setembro de 2019, de https://www.govtrack.us/congress/bills/100/s2361.

[59] A Lei de Proteção e Concorrência da Televisão a Cabo de 1992, também conhecido como 1992 Cable Act, é um Lei federal dos Estados Unidos que exigiu Televisão à cabo sistemas para transportar a maioria das transmissões locais canais de televisão e as operadoras de cabo proibidas de cobrar das emissoras locais para transportar seu sinal. Recuperado em 12 de setembro de 2019, de https://www.congress.gov/bill/102nd-congress/house-bill/4850.

[60] A Lei de Proteção ao Crédito ao Consumidor protege as informações coletadas por agências de relatórios ao consumidor, como agências de crédito, empresas de informações médicas e serviços de triagem de inquilinos. As informações em um relatório do consumidor não podem ser fornecidas a ninguém que não tenha uma finalidade especificada na lei. As empresas que fornecem informações às agências de informação ao consumidor também têm obrigações legais específicas, incluindo o dever de investigar as informações contestadas. Além disso, os usuários das informações para fins de crédito, seguro ou emprego devem notificar o consumidor quando uma ação adversa for tomada com base em tais relatórios. A Lei de Transações de Crédito Justas e Precisas adicionou muitas disposições legais principalmente a temas relacionados à precisão de registros e roubo de identidade. Recuperado em 13 de setembro de 2019, de https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf.

Como resultado, não há, da mesma forma, como notado por Guidi (2018) uma estrutura constitucional sobre a qual construir uma única lei de privacidade de dados, tornando a abordagem "*ad hoc"* muito mais compatível com o sistema de governo americano.

Os Estados Unidos da América, em comparação com a União Europeia, na perspectiva de Guidi (2018) legislam sobre privacidade de dados de maneira diferente da União Europeia e não têm uma lei abrangente de proteção de dados como o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da UE. De acordo com guias jurídicos comparativos internacionais, os EUA têm uma variedade de leis federais e estaduais que visam proteger a privacidade e os dados *online* de um cidadão. Não existe uma grande parte da legislação governando em nível nacional, mas, ao contrário, uma miscelânea de leis federais e estaduais que atendem a esse propósito.

No entanto, a abordagem de Foxx (2018), em que a ideia de criar uma grande parte da legislação semelhante ao Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia não está fora de questão. Muitos legisladores propuseram uma nova legislação federal em uma tentativa de expandir as proteções de privacidade de dados presentes nas leis dos EUA. Observa-se que em fevereiro de 2020, uma nova proposta da senadora democrata do estado de Nova York, Kirsten Gillibrand, recomendou a criação de uma nova Agência de Proteção de Dados (Foxx, 2018).

Essa nova agência federal seria encarregada de fazer cumprir os regulamentos de privacidade de dados dos Estados Unidos da América e de conduzir investigações sobre possíveis violações dessas proteções (Foxx, 2018). No entanto, as preocupações e necessidades dos atores da indústria e da comunidade empresarial são igualmente importantes quando se considera esses tipos de legislação.

Organizações como a "*Privacy for America*"[61] segundo Foxx (2018), que representa um conglomerado de órgãos do setor em privacidade de dados, trabalham para garantir que qualquer nova legislação aprovada nos EUA leve em consideração as necessidades do setor.

[61] A Privacy for America trabalha com o Congresso Norte Americano para apoiar a aprovação de uma legislação federal abrangente de privacidade e segurança de dados do consumidor. Descrevendo um novo paradigma ousado para uma lei nacional que tornaria os dados pessoais menos vulneráveis a violação ou uso indevido e estabeleceria proteções de privacidade do consumidor claras, exequíveis e em todo o país pela primeira vez. Recuperado em 20 de setembro de 2019, de https://www.privacyforamerica.com/about/.

Os Estados Unidos da América, continuam a enfatizar os direitos dos estados em seu governo e sua abordagem de baixo para cima, e à privacidade de dados conduz a essa ênfase a ser abordada em suas legislações e normas legais (Soprana, 2018).

A União Europeia por outro lado, adotou uma abordagem de cima para baixo em relação à privacidade de dados, enquanto os Estados Unidos da América adotaram uma abordagem mais de baixo para cima (Soprana, 2018). Depois de se examinar os dois sistemas, essa diferença de abordagem não casou surpresa. A União Europeia foi uma instituição fundada em um equilíbrio de políticas intergovernamentais e supranacionais e, neste caso, sua abordagem à privacidade de dados é supranacional.

Estes dois entes políticos gigantescos, a União Europeia e os Estados Unidos da América, como evidenciados pela pesquisa de Soprana (2018) têm duas abordagens muito díspares para manter a privacidade de dados e a proteção de seus cidadãos.

Em última análise, essas duas entidades estão em lugares muito diferentes em termos de legislação de privacidade de dados. A União Europeia tem agora uma legislação abrangente, tornou a privacidade de dados uma prioridade clara e, como resultado, continua a desenvolver essa legislação com o passar do tempo. Os Estados Unidos da América, por outro lado, ainda estão procurando sua solução de cima para baixo e podem encontrá-la na criação de uma nova agência federal (Soprana, 2018).

Ao contrário de outras jurisdições, os Estados Unidos da América não têm uma única lei de proteção de dados em nível federal, mas regulamenta a privacidade principalmente pela indústria, setor por setor. Existem inúmeras fontes de leis de privacidade nos EUA, incluindo leis e regulamentos desenvolvidos em nível federal e estadual, enfatiza Proxxima, (2018) em seu trabalho. Essas leis e regulamentos podem ser aplicados por autoridades federais e estaduais, e muitos fornecem aos indivíduos o direito privado de entrar com ações judiciais contra organizações que acreditam estarem violando a lei.

A partir de 2018, o aumento da atividade legislativa em nível estadual sinalizou uma mudança no foco em direção a uma legislação de privacidade do consumidor mais ampla nos Estados Unidos da América. A Califórnia se tornou o primeiro estado a promulgar tal legislação com a aprovação do a Lei de Privacidade do Consumidor da Califórnia, uma ampla lei de privacidade inspirada em parte pelo Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia, que visa proteger informações pessoais de consumidores em toda a indústria como ressaltou Doneda & Córdova (2018). Desde então, vários outros estados propuseram uma legislação de privacidade igualmente ampla,

enquanto vários projetos de lei de privacidade abrangentes foram apresentados em nível federal no Congresso dos Estados Unidos da América.

O escopo do California Consumer Privacy Act de 2018[62], sigla em inglês da Lei de Privacidade do Consumidor da Califórnia que é um dos principais faróis deste tipo de legislação o contrário das disposições federais diversas, nem o método de coleta de dados nem o setor em que a empresa opera limita a aplicação potencial do CCPA. Em vez disso, a California Consumer Privacy Act se aplica a qualquer empresa que coleta informações pessoais de californianos, tem fins lucrativos, faz negócios na Califórnia e atende a um conjunto básico de limites (Doneda & Córdova, 2018).

A CCPA (2018) adotou um conceito bastante semelhante ao conceito de controlador do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), em que os negócios diretamente sujeitos à lei são definidos como as entidades que determinam os fins e os meios de tratamento dos dados pessoais dos consumidores (Doneda & Córdova, 2018).

O tema, como apontado por Doneda & Córdova (2018) que convergem nas áreas jurídicas e de novas tecnologias sugere que esses limites são baixos o suficiente para que a lei consiga atingir um número considerável de empresas, até mesmo as relativamente pequenas com sites acessíveis na Califórnia[63].

A California Consumer Privacy Act (2018) também não faz distinção entre as fontes de dados que entram em seu escopo. Em vez disso, regula todas as informações pessoais que, pela definição da CCPA[64], abrangem quase todas as informações que uma empresa coletaria de um consumidor.

---

[62] A Lei de Privacidade do Consumidor da Califórnia ou California Consumer Privacy Act de 2018 (CCPA) oferece aos consumidores mais controle sobre as informações pessoais que as empresas coletam sobre eles e os regulamentos da CCPA fornecem orientação sobre como implementar a lei. Esta lei histórica garante novos direitos de privacidade para os consumidores da Califórnia. Recuperado em 25 de setembro de 2019, de https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[63] Christopher A.O. (2018). *Q&A: Privacy and Security Partner Christopher Ott on the California Consumer Privacy Act of 2018*. Privacy & Security Law Blog. Recuperado em 09 de novembro de 2019, de https://www.privsecblog.com/2018/08/articles/marketing-andconsumer-privacy/qa-privacy-and-security-partner-christopher-ott-on-the-california-consumer-privacy-act-of-2018/.

[64] *Código Civil da Califórnia § 1798.140 (c)*. "A CCPA se aplica a informações pessoais amplamente definidas de residentes da Califórnia coletadas por empresas, independentemente de como a coleta é feita ou do tipo de indústria em que a empresa opera.".

A lei não exige a presença de nenhum identificador individual, como um nome ou endereço, para que os dados se enquadrem no significado de informações pessoais, aborda Doneda (2018) sobre este assunto. Em vez disso, a California Consumer Privacy Act (2018) define amplamente as informações pessoais como informações que identificam, se relacionam com, descrevem ou podem ser associadas, ou podem estar razoavelmente vinculadas, direta ou indiretamente, a um determinado consumidor ou família[65].

Seguindo esta definição, a California Consumer Privacy Act (2018) fornece algumas ilustrações reveladoras do que constitui informação pessoal, incluindo qualquer atividade de rede eletrônica como histórico de navegação, histórico de pesquisa e informações sobre a interação de um consumidor com um *site*, aplicativo ou anúncio da Internet e inferências tiradas de qualquer uma dessas informações[66].

As disposições e requisitos da California Consumer Privacy Act (2018) fornece aos consumidores três "direitos" principais como ressalta Doneda (2018). O primeiro deles é o "direito de saber" as informações que as empresas coletaram ou venderam sobre seus usuários. Este direito exige que as empresas devem, antes de qualquer coleta, informar por correio ou eletronicamente os consumidores sobre as categorias de informações pessoais a serem coletadas e os fins para os quais as informações serão destinadas, o California Consumer Privacy Act ainda fornece aos consumidores o direito de optar pela venda de informações do consumidor.

De acordo com a lei, as empresas devem informar os consumidores deste direito, e se um consumidor desistir afirmativamente, a empresa não pode vender novamente as informações do consumidor, a menos que o consumidor posteriormente forneça autorização expressa à empresa[67].

Por fim, a California Consumer Privacy Act (2018) concede aos consumidores o direito, em certas circunstâncias, de solicitar que uma empresa exclua qualquer informação

---

[65] *Código Civil da Califórnia § 1798.140(O)(1).*

[66] *Código Civil da Califórnia § 1798.140(O)(1)(A)–(K).* A CCPA isenta algumas categorias de informações de sua definição de informações pessoais. Por exemplo, informações pessoais geralmente não incluem "informações publicamente disponíveis", ou seja, informações legalmente disponibilizadas a partir de registros governamentais. Da mesma forma, a CCPA não restringe a capacidade de uma empresa de coletar. "informações desidentificadas" ou "agregadas ao consumidor", geralmente significando informações que não podem ser vinculadas de forma alguma a consumidores específicos. As obrigações impostas às empresas por este título não devem restringir a capacidade de uma empresa.

[67] *Código Civil da Califórnia § 1798.120.*

coletada sobre o consumidor, ou seja, o direito de exclusão como observa Doneda & Córdova (2018). De acordo com a lei, uma empresa que recebe tal solicitação deve excluir as informações coletadas e orientar seus prestadores de serviço a fazer o mesmo[68].

Além dos requisitos da Lei de Proteção à Privacidade *Online* da Califórnia, a California Consumer Privacy Act exige que as empresas notifiquem os consumidores sobre seus direitos sob a Lei conforme destaca Doneda & Córdova (2018), por exemplo, o direito de recusar a venda de informações pessoais, obter uma lista das categorias de informações pessoais coletadas sobre consumidores nos 12 meses anteriores a solicitação e, quando aplicável, que a empresa evidencie as pratica de venda ou divulga de suas informações ou dados pessoais.

Se a empresa vende informações pessoais de consumidores ou as divulga a terceiros para fins comerciais, o aviso também deve incluir lista das categorias de informações pessoais vendidas e divulgadas sobre os consumidores, respectivamente (Doneda & Córdova, 2018).

As empresas, ressaltando agora a apreciação de Determann (2018) devem fornecer separadamente um *link* claro e visível em seu *site* alertando de forma clara a opção de não venda de informações pessoais e fornecer aos consumidores um mecanismo para recusar a venda de suas informações pessoais, uma decisão que a empresa deve respeitar. As empresas devem atualizar seus avisos pelo menos uma vez a cada doze meses.

Delaware e Nevada como aponta Determann, (2018) também promulgaram leis que exigem que os operadores de serviços comerciais de Internet forneçam informações semelhantes a seus usuários ao coletar informações de usuários online. Além das leis da Califórnia, Delaware e Nevada, existem outras leis federais que exigem que um aviso de privacidade seja fornecido em determinadas circunstâncias.

As leis em vários estados dos EUA, incluindo a Califórnia, impõem padrões gerais de segurança da informação às organizações que mantêm informações pessoais. A lei da Califórnia, por exemplo, exige que as organizações que possuem ou licenciam informações pessoais sobre os residentes da Califórnia implementem e mantenham procedimentos e práticas de segurança razoáveis para proteger a segurança das informações contra acesso não autorizado, destruição, uso, modificação ou divulgação (Determann, 2018).

[68] *Código Civil da Califórnia § 1798.105.*

Além disso, as organizações que divulgam informações pessoais a terceiros não afiliados a um serviço devem exigir contratualmente que essas entidades mantenham procedimentos de segurança razoáveis (Determann, 2018).

Em 2008, ainda na senda de Determann (2018), o estado de Massachusetts emitiu padrões de regulamentos exigindo que qualquer pessoa que detém informações pessoais sobre os residentes de Massachusetts desenvolva e implemente um programa de segurança de informações por escrito, que seja abrangente para proteger os dados e a segurança da informação.

Os regulamentos aplicam-se tanto no contexto de informações de consumidores quanto de funcionários e exigem a proteção de dados pessoais em papel e em formato eletrônico como lembra Proxxima (2018). Ao contrário da lei da Califórnia, a lei de Massachusetts contém certos padrões de segurança de dados específicos, incluindo proteções técnicas exigidas, em todas as entidades privadas com consumidores ou funcionários de Massachusetts.

Já o Regulamento de Segurança Cibernética[69] do Departamento de Serviços Financeiros de Nova York (NYDFS[70]) por exemplo, que em 2017 emitiu uma norma que estabelece um conjunto robusto de requisitos de segurança cibernética para prestadores de serviços financeiros regulamentados pelo NYDFS. O regulamento de segurança cibernética conforme destaca Elias (2018) se aplica a entidades que operam sob uma licença, registro

[69] O Regulamento de Cibersegurança NYDFS (23 NYCRR 500) é um novo conjunto de regulamentos do Departamento de Serviços Financeiros de NY (NYDFS) que impõe requisitos de cibersegurança a todas as instituições financeiras cobertas. As regras foram lançadas em 16 de fevereiro de 2017 após duas rodadas de feedback da indústria e do público e incluem 23 seções que descrevem os requisitos para desenvolver e implementar um programa de segurança cibernética eficaz, exigindo que as instituições cobertas avaliem seus riscos de segurança cibernética e desenvolvam planos para abordar de forma proativa esses riscos. O regulamento de segurança cibernética do NYDFS incluiu um processo de implementação em fases, com quatro fases distintas, permitindo que as organizações tenham tempo para implementar políticas e controles mais robustos. Recuperado em 25 de novembro de 2019, de https://ccl.yale.edu/sites/default/files/files/New%20York%20State%20Department%20of%20Financial%20Services%20-%20Cybersecurity%20Requirements.pdf.

[70] O New York State Department of Financial Services (DFS or NYSDFS) é o departamento do governo do estado de Nova York responsável por regulamentar os serviços e produtos financeiros, incluindo aqueles sujeitos às leis de seguros, bancos e serviços financeiros de Nova York. Recuperado em 27 de novembro de 2019, de https://www.dfs.ny.gov/.

ou alvará do NYDFS de acordo com as leis de serviços bancários, de seguros ou financeiros de Nova York.

O Regulamento de Segurança Cibernética como bem lembra Elias (2018) exige que tais entidades submetidas a este regulamento mantenham um programa de segurança cibernética abrangente e implementem certos processos e controles técnicos relacionados a avaliações de risco, privilégios de acesso de usuário, segurança de *software*, auditoria e monitoramento de sistema, criptografia de dados, eliminação e retenção de dados e protocolos para incidente de falha de segurança cibernética, além da sua imediata resposta bem como do restabelecimento da segurança de informações e dados.

Dado o impacto econômico significativo da legislação da Califórnia e o fato de que a CCPA (2018) é a lei geral de privacidade mais significativa no cenário jurídico da proteção de dados dos Estados Unidos da América, a lei ajudou a preparar o terreno para uma série de propostas de códigos e normas com foco semelhante, atualmente pendentes nas legislaturas estaduais, bem como uma possível lei federal de privacidade de dados. Se uma lei federal prevalecerá sobre as leis estaduais, como a Lei de Privacidade do Consumidor da Califórnia, também é um assunto de debate e estudo como adverte Proxxima (2018) visto a ainda pouca literatura jurídica sobre a temática em questão.

3.4.2 O Canadá

No Canadá, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos ou Personal Information Protection and Electronic Documents Act (PIPEDA, 2000)[71] é a principal fonte de regulamentação que rege o gerenciamento de dados pessoais.

PIPEDA[72], ou Lei de Proteção de Informações Pessoais e Documentos Eletrônicos em inglês, visa apoiar e promover o comércio eletrônico, principalmente protegendo os dados pessoais que são coletados, usados ou transmitidos neste contexto como observou Szeto & Miri (2007) em sua pesquisa. Os dados aos olhos da legislação canadense são uma forma de representação das informações, sejam elas manuais ou eletrônicas. Um documento eletrônico é uma forma de representação de informações.

[71]Recuperado em 07 de fevereiro de 2020, de https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

[72] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Aprovado para 13/04/2000; Recuperado em 07 de fevereiro de 2020, de https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

A estrutura do PIPEDA em termos gerais, a seção 4 do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) estabelece que se aplica a organizações[73] e às informações pessoais[74] que elas coletam, usam ou divulgam no curso de atividades comerciais[75]. Em suas definições gerais, no âmbito do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000), várias expressões-chave são utilizadas, fornecendo ao cidadão comum breves definições do que cada um desses elementos representa aos olhos da lei. Uma informação pessoal representa para um indivíduo, vivo ou falecido, todas as informações que permitem reconhecer a sua identidade e que não garantem o seu anonimato (Szeto & Miri, 2007).

Cada um dos termos entre aspas é definido separadamente na legislação. Cada um também é definido de forma abrangente, dando ao Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) uma ampla aplicação para atores do setor privado em sua coleta, uso e divulgação de informações pessoais. O Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) também segundo Szeto & Miri (2007) se aplica às informações pessoais que são sobre um funcionário da organização e que a organização coleta, usa ou divulga em conexão com a operação de uma obra, empreendimento ou negócio de âmbito federal[76].

Apesar do seu amplo escopo, certas atividades estão excluídas da aplicação do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000). Por exemplo, para evitar conflito com a Lei de Privacidade Canadense[77], a aplicação do PIPEDA ao setor público federal é expressamente excluída[78].

O Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) também não se aplica a qualquer indivíduo em relação a informações pessoais que o

---

[73] Uma organização é definida como: "uma associação, uma parceria, uma pessoa e um sindicato". (PIPEDA, nota supra 1, s. 2).

[74] "Informações pessoais são definidas como "informações sobre um indivíduo identificável, mas não incluem o nome, cargo ou endereço comercial ou número de telefone de um funcionário de uma organização". PIPEDA, 2000.

[75] PIPEDA, ibid., S. 4 (1) (a). "A atividade comercial é definida como qualquer transação, ato ou conduta particular ou qualquer curso regular de conduta que seja de caráter comercial, incluindo a venda, troca ou arrendamento de doadores, membros ou outras listas de arrecadação de fundos ". PIPEDA, 2000.

[76] PIPEDA, ibid., s. 4(1)(b).

[77] RSC 1985, c. P-21.

[78] PIPEDA, ibid., s. 4(2)(a).

indivíduo coleta, usa ou divulga para fins pessoais ou para fins domésticos e não coleta, usa ou divulga para qualquer outro fim[79] (Szeto & Miri, 2007).

Em certo sentido, esta exclusão apenas reforça que o Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) se aplica exclusivamente à coleta, uso ou divulgação de informações pessoais no curso de atividades comerciais. Atividades puramente pessoais ou domésticas estão fora de seu escopo.

A aplicação da Lei também está expressamente excluída no caso de qualquer organização em relação às informações pessoais que a organização coleta, usa ou divulga para fins jornalísticos, artísticos ou literários e não coleta, usa ou divulga para qualquer outra finalidade[80]. Esta exceção, sem dúvida, visa equilibrar segundo Szeto & Miri (2007) os direitos de privacidade dos indivíduos em suas informações pessoais com os valores de liberdade de expressão.

À parte essas exceções, as disposições normativas do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) recebem ampla aplicação para a coleta, uso ou divulgação de informações pessoais por atores do setor privado no curso de atividades comerciais.

As informações pessoais de saúde, por exemplo, no âmbito da proteção de informações de um cidadão que está amparado por um regime constitucional, representam para um indivíduo, vivo ou falecido todas as informações sobre sua saúde mental ou física, todas as informações relacionadas a um ou mais cuidados de saúde prestados a ele, todas as informações relacionadas com exames médicos ou resultados analíticos, todas as informações coletadas como parte de um serviço de saúde que utiliza cadastro e proteções de dados e informações sensíveis ou de caráter pessoal (Szeto & Miri, 2007).

Os dados são registrados ou armazenados em um computador e podem ser lidos por um indivíduo ou por um sistema informatizado seguindo Szeto & Miri (2007), onde podemos perceber que tais valores protegidos pelo ordenamento jurídico canadense estão em harmonia com o ordenamento europeu baseando-se na pesquisa de Castro (2005). Por associação a essa linha de pensamento, um documento eletrônico também inclui dispositivos de exibição tais como telas, tablets e outros dispositivos eletrônicos que tem a capacidade de arquivar dados, assim como impressão e saída de dados como em discos externos, além de dispositivos de armazenamento em geral de acordo com PIPEDA (2000).

---

[79] PIPEDA, ibid., s. 4(2)(b).

[80] PIPEDA, ibid., s. 4(2)(c).

Os princípios para a proteção de informações pessoais buscam estabelecer pontos específicos como a Responsabilidade das organizações, em que são todas responsáveis pelas informações e dados pessoais que possuem e devem designar uma ou mais pessoas encarregadas da conformidade regulatória da organização. A identidade dessas pessoas designadas pela organização para garantir essa conformidade deve estar disponível mediante solicitação do titular dos dados (Szeto & Miri, 2007).

A delimitação das finalidades da colheita de informações, está na compreensão de que as informações pessoais coletadas devem ser identificadas pela organização no momento em que as informações são angariadas, ou antes mesmo. A organização deve documentar as finalidades para as quais as informações e os dados pessoais são coletados, a fim de respeitar o princípio da transparência e do acesso às informações das pessoas envolvidas de acordo com as normas estabelecidas pelo PIPEDA (2000).

Já quanto ao consentimento segundo Szeto & Miri (2007), o indivíduo deve ser informado claramente sobre a finalidade da coleta e dar seu consentimento livre e esclarecido[81]. A forma de consentimento fornecida pode variar de acordo com as circunstâncias e o tipo de informação, podendo ser concedido de várias maneiras, como na forma de formulário, na forma de *checkbox*, na forma oral, se a informação for recolhida por telefone ou no momento em que os indivíduos, utilizando um produto ou serviço, são contactados por telefone para cobrança. Este princípio de consentimento deve indiscutivelmente ser de forma clara ao titular dos dados, observando o que pode ser dispensado em casos que não se mostre necessário.

Lembrando que a limitação da coleta de informações pessoais, esta deve ser estritamente restrita ao necessário para os fins determinados pela organização durante a fase de delimitação dos objetivos da coleta de dados. As informações também devem ser coletadas por meios justos e legais como prega o PIPEDA (2000). Geralmente, quanto mais informações confidenciais forem consideradas, mais rigorosos serão os requisitos de consentimento[82].

A Limitação de uso, divulgação e retenção das informações e dados pessoais não devem ser usadas ou divulgadas para fins diferentes daqueles para os quais foram coletados, exceto com o consentimento do indivíduo em questão ou se a lei assim exigir. Além disso, essas informações pessoais só devem ser mantidas até o cumprimento dos propósitos

[81] PIPEDA, supra note 1, Schedule I, Clause 4.3.2.

[82] PIPEDA, ibid., Schedule I, Clause 4.3.6.

estabelecidos. Assim que for concluído, as informações devem ser destruídas (Szeto & Miri, 2007).

No que diz respeito a exatidão das informações pessoais Szeto & Miri (2007) ressalta que estas devem ser precisas, completas e atualizadas, conforme necessário para os fins em que tais dados serão utilizados. Quanto as medidas de proteção: As informações pessoais devem ser protegidas respeitando o grau de sensibilidade dos dados PIPEDA (2000).

Passando a questão voltada a transparência das organizações, ela deve disponibilizar prontamente aos indivíduos informações específicas sobre suas políticas e práticas com relação à aplicação do gerenciamento de informações pessoais[83] PIPEDA (2000).

No direito de acesso, um indivíduo deve poder, mediante simples solicitação, ter acesso às informações pessoais que lhe dizem respeito e poder contrapor sua veracidade e solicitar modificações, se necessário, sendo também possível o direito de contestar, devendo ser capaz de contatar o responsável pelo *compliance*[84] e a gestão de dados dentro de uma organização e informá-lo de sua contestação em relação aos princípios acima mencionados (Szeto & Miri, 2007).

Na estrutura atual do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000), o consentimento não é necessário para a coleta, uso ou divulgação de informações pessoais que estão disponíveis publicamente. Os regulamentos que especificam as informações publicamente disponíveis contêm uma lista fechada de fontes de informações que podem ser consideradas publicamente disponíveis (Szeto & Miri, 2007).

Os Regulamentos são redigidos de forma restrita e também é claro que a exceção à regra de consentimento para informações publicamente disponíveis, no qual se configura apenas quando tais informações são coletadas, usadas ou divulgadas para os fins dos quais foram disponibilizadas de forma pública, ou para fins em que uma pessoa consideraria apropriados em determinadas circunstancias em que estes dados foram a público[85].

---

[83] Algumas dessas finalidades são abordadas no "Guidance Document, Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals", 2010, online. Recuperado em 11 de fevereiro de 2020, de http://www.priv.gc.ca/information/pub/gd_trib_201002_e.cfm.

[84] Compliance é a prática de obedecer a regras ou solicitações feitas por pessoas em posição de autoridade. Recuperado em 05 de outubro de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/compliance.

[85] Alberta Regulation, supra note 58, s. 7(e).

As informações públicas ainda são informações pessoais e, no contexto da proteção de dados, o principal objetivo é fornecer aos indivíduos alguma medida de controle sobre o uso de suas informações pessoais por organizações do setor privado (Celeste, 2019).

Atualmente, pode ser possível argumentar que algumas informações "*postadas"* em sites de redes sociais ou em outros contextos da Internet pelo titular dos dados podem se enquadrar em uma das categorias existentes de informações publicamente disponíveis. Por exemplo, as informações postadas em um *site* como o *LinkedIn* podem ser consideradas informações em um diretório profissional ou comercial. As informações postadas em blogs ou em um site como o *Facebook* podem ser consideradas uma "*publicação*" (Bioni, 2019).

No entanto, Szeto & Miri (2007) lembra que há boas razões para não interpretar essas categorias nos Regulamentos de forma ampla a ponto de incluir todas essas fontes de informações pessoais. Não está claro se todos os sites de redes sociais estão genuinamente fontes disponíveis de informações que deviam ser encarados como um dado que pode ou deve ser exposto publicamente[86].

Em vez de abrir os movimentos dos indivíduos através do espaço público real ou virtual para a coleta irrestrita de dados, uma abordagem melhor seria considerar se as exceções existentes ao consentimento, estabelecidas na seção 7 do Personal Information Protection and Electronic Documents Act (PIPEDA, 2000), são suficientes para atender às necessidades legítimas das empresas, e para satisfazer o interesse público dos usuários em geral (Szeto & Miri, 2007).

Hoje, essas exceções permitem a coleta, uso ou divulgação de informações pessoais para uma ampla gama de finalidades, incluindo cobrança de dívidas, conceções de credito bancário, situações de emergência, quando há uma ordem judicial ou para investigações[87], logo a relação entre o Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) e suas contrapartes provinciais substancialmente semelhantes deve ser mantida em mente ao considerar as reformas do PIPEDA (2000) ou mudanças em suas contrapartes substancialmente semelhantes (Bioni, 2019).

Pode ser confuso e perturbador para o bom funcionamento das normas ou limites de proteção de dados muito diferentes de uma província para outra. Sem dúvida, seguindo o pensamento analítico de Bioni (2019) existem diversas maneiras de melhorar, reformar ou

[86] section 7 of PIPEDA, supra note 1.

[87] Online Tracking, supra note 26 at 17.

corrigir os estatutos, de forma que não mudem drasticamente seu escopo ou seus princípios normativos fundamentais que levaram a sua origem.

No entanto, conforme Celeste (2019) uma mudança nos regulamentos que regem as informações publicamente disponíveis que incluem sites de redes sociais ou informações reveladas em contextos públicos seria significativo e faria com que essas informações fossem tratadas de maneira muito diferente em uma jurisdição do que em outra, observando o as regras delimitadas no PIPEDA.

3.4.3 A República Federativa do Brasil

Os princípios e disposições gerais sobre proteção de dados e privacidade no Brasil podem ser derivados da Constituição Federal de 1988[88], do Código Civil Brasileiro de 2002[89] e estatutos e regulamentos que tratam de tipos específicos de relações públicas e privadas, de diferentes setores, por exemplo, instituições financeiras, indústria da saúde, o setor de telecomunicações, e o tratamento e acesso a documentos e informações administrados por entidades e órgãos governamentais (Gonçalves, 2017). Dentre esses estatutos, os mais importantes são o Código do Consumidor[90] e o Marco Civil da Internet[91].

Em termos gerais, a Constituição Federal Brasileira de outubro de 1988 protege o direito à privacidade, incluindo o sigilo da correspondência, telégrafo, telefone e comunicação de dados (Brasil, 1988).

Também existem mecanismos legais que permitem o acesso à informação. Em resposta às demandas sociais, após o fim do regime militar vigente no país, a Constituição também concedeu acesso a informações pessoais coletadas por órgãos governamentais. Esse acesso foi viabilizado por meio do Mandado de *Habeas Data*, instituído na Constituição de 1988 e regulamentado pela Lei nº 9.507 de 1997[92] que versa sobre o acesso a um *Habeas*

---

[88] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Recuperado em 17 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

[89] LEI N o 10.406, DE 10 DE JANEIRO DE 2002. Institui o Código Civil. Recuperado em 17 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

[90] *Código de Defesa do Consumidor - Lei 8.078 DE 1990.* Dispõe sobre a proteção do consumidor e dá outras providências.

[91] *Lei 12.965 de 2014.* Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

[92] Regula o direito de acesso a informações e disciplina o rito processual do habeas data, que considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser

Data. O documento influenciou outros países latino-americanos que implementaram instrumentos de proteção de dados semelhantes (Santos, 2018).

O mandado de *Habeas Data*, como bem ressaltou Santos (2018) consiste em uma medida constitucional, que pode ser utilizado para permitir o acesso às informações relativas ao indivíduo armazenadas em bancos de dados governamentais ou públicos, para corrigir ou atualizar dados, também para proceder as anotações ou esclarecimentos em bancos de dados públicos sobre litígios pendentes. Uma gravação de *Habeas Data* pode ser endereçada a qualquer banco de dados que coleta informações que são ou podem ser transmitidas a terceiros, bem como informações que não são utilizadas exclusivamente pelo órgão governamental ou entidade legal que gerou ou gerencia essas informações.

No entanto, o mandado de *Habeas Data* é um remédio caro e lento porque uma petição deve ser apresentada por um advogado após uma solicitação de dados sem sucesso do réu (Gonçalves, 2017). O mandado não é considerado uma ferramenta moderna de proteção de dados nem se desenvolveu como tal. Em vez disso, outros instrumentos foram desenvolvidos na legislação brasileira para abordar o uso crescente do processamento eletrônico de dados. Esses instrumentos incluem o Lei de Informação de Crédito[93] e a Lei de Acesso à Informação[94].

A Constituição Federal Brasileira (1988), também se refere diretamente à proteção do consumidor, tanto no seu Artigo 5º, XXXII[95], que considera a proteção do consumidor um direito fundamental, quanto no Artigo 170, V[96], que estabelece a proteção do consumidor como princípio da ordem econômica nacional, bem como no Artigo 48 de disposições

---

transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações.

[93] 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.

[94] Versa sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal Brasileira.

[95] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Art. 5º, XXXII; "o Estado promoverá, na forma da lei, a defesa do consumidor". Recuperado em 18 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

[96] CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios; V - defesa do consumidor; Recuperado em 18 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

transitórias que criam a obrigação de promulgar um Código Brasileiro de Defesa do Consumidor (2017)[97].

Esse Código, observando a obra de Santos (2018) em particular, fornece uma estrutura multifacetada para tratar de questões de proteção ao consumidor e equilibrar as informações e assimetrias de poder entre consumidores e empresas. Isso envolve uma variedade de normas baseadas em princípios, mas que não eram amplas o suficiente para oferecer soluções para novos conflitos relacionados à tecnologia da informação e à proteção dos direitos de privacidade ao qual estamos expostos com as novas mídias e tecnologias.

O Código Civil Brasileiro (2002) por sua vez se aplica às relações privadas envolvendo pessoas físicas e jurídicas. Os atos de proteção de dados no Brasil costumavam ser setoriais e regulamentar questões específicas como proteção ao consumidor, telecomunicações, Internet, sendo aplicáveis apenas a um determinado setor. Havia uma disposição geral de proteção de dados aplicável apenas no que diz respeito ao acesso a informações pessoais e sua eventual retificação (Santos, 2018).

Mas, em agosto de 2018, foi emitida a Lei Geral de Proteção de Dados (LGPD, 2018), que entrou em vigor no início de 2020 (Guidi, 2018). Ela cria um arcabouço legal de proteção de dados pessoais no Brasil, com aplicação geral, incluindo os setores público e privado, e substituindo ou ampliando as existentes leis setoriais.

Bioni (2019), em uma ampla pesquisa sobre Lei Geral de Proteção de Dados (LGPD, 2018) mostra que esta cobre uma série de questões, como um forte conjunto de princípios, regras para aplicação extraterritorial, disposições de segurança sólidas, regulamentação de transferências de dados transfronteiriças, obrigações de nomear funcionários de proteção de dados e realizar avaliações de impacto da proteção de dados, entre outras características positivas que são frutos de anos de engajamento público e de uma sociedade civil atuante no processo. Estas disposições uniformizam e complementam o quadro de proteção de dados existente, resolvendo questões como a aplicação extraterritorial das Leis de Proteção de Dados, que era uma lacuna comum antes da aprovação da LGPD de 2018.

[97] LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor. Recuperado em 18 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

A Lei Geral de Proteção de Dados (LGPD, 2018)[98] cria um novo arcabouço legal para o uso de dados pessoais no Brasil, tanto online quanto offline, nos setores público e privado. É importante destacar que o país já possui mais de 40 normas jurídicas em âmbito federal que tratam direta e indiretamente da proteção da privacidade e dos dados pessoais em um sistema setorial (Bioni, 2019). No entanto, a Lei Geral de Proteção de Dados (LGPD, 2018) está a substituir ou complementar este quadro regulamentar setorial, por vezes conflituoso, pantanoso, sem segurança jurídica e que tornou o país menos competitivo num contexto de uma sociedade cada vez mais orientada para os fluxos constantes de dados e informações que são disponibilizados pela globalização tecnológica.

O texto base, fruto de uma ampla discussão, visa não só garantir os direitos individuais, mas também fomentar o desenvolvimento econômico, tecnológico e da inovação por meio de regras claras, transparentes e abrangentes para o uso adequado dos dados pessoais (Bioni, 2019). Por ter uma Lei Geral de Proteção de Dados (LGPD, 2018), o Brasil entra no rol de mais de 120 países que hoje podem ser considerados como tendo um nível adequado de proteção da privacidade e do uso de dados pessoais de maneira segura conforme observa Bioni (2019).

Seguindo com esta interpretação, é possível notar o principal objetivo desta legislação, que se mostra logo no primeiro artigo da Lei Geral de Proteção de Dados (LGPD, 2018) que versa (Brasil, 2018):

> 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.

A Lei Geral de Proteção de Dados (LGPD, 2018) tem aplicação transversal e multissetorial, tanto no setor público como no privado, *online* e *offline*. Aborda o conceito de dados pessoais e enumera as bases jurídicas que autorizam a sua utilização, e o consentimento é apenas uma delas, destacando a possibilidade de tratamento de dados pessoais e sensíveis com base nos legítimos interesses do responsável pelo tratamento, além dos princípios gerais de proteção de dados; direitos básicos do titular dos dados e

[98] LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado em 20 de julho de 2019, de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

informações, como direito de acesso, exclusão de dados e explicação de quais dados foram colhidos; e as obrigações e limites que devem ser aplicados a qualquer entidade que processe dados ou informações pessoais e sensíveis (Guidi, 2018).

Quanto a aplicação extraterritorial, de forma semelhante ao Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia, a Lei Geral de Proteção de Dados (LGPD, 2018) terá esta característica de aplicação em ambiente de extraterritorialidade, ou seja, o dever de conformidade ultrapassará os limites geográficos do Brasil (Guidi, 2018). Qualquer empresa estrangeira que tenha pelo menos uma filial no Brasil, ou ofereça serviços para o mercado brasileiro e colete e trate dados pessoais de titulares de dados localizados no país, independentemente da nacionalidade, estará sujeita à nova lei.

No seu conceito ainda seguindo o pensamento de Guidi (2018) de dados pessoais a Lei Geral de Proteção de Dados (LGPD, 2018) fornece um conceito amplo do que deve ser considerado dado pessoal relacionado a uma pessoa física identificada ou identificável. Ou seja, quaisquer dados, isolados ou agregados a outro, que possam permitir a identificação de uma pessoa física ou sujeitá-la a determinado comportamento ou interpretação possível a partir de uma leitura integrativa do arquivo de dados ou informações.

Nesta época de *'Big Data*', que permite a correlação rápida de grandes bancos de dados estruturados e não estruturados, praticamente qualquer dado pode eventualmente ser considerado pessoal, portanto, sujeito à Lei (Celeste, 2019).

Já o conceito de dados pessoais sensíveis consiste em caracterizar os dados pessoais sensíveis como dados ou informações que, pela sua própria natureza, podem sujeitar o titular dos dados a práticas discriminatórias, tais como dados sobre origem racial ou étnica, crença religiosa, opinião política, dados de saúde ou vida sexual, ou permite a identificação inequívoca e persistente do titular dos dados, como dados genéticos, isto com ambas as facetas, discriminação e identificação ou biométricos (Mendes & Mattiuzzo, 2019).

Esses dados devem ser tratados de forma diferenciada conforme Gellert (2018), com camadas de segurança adicionais e com bases jurídicas diversas, como o consentimento expresso do titular dos dados.

Se tratando de dados anônimos a Lei Geral de Proteção de Dados (LGPD, 2018) referem-se a informações sobre um titular dos dados que não podem ser identificados considerando o uso de tempo, custo e meios técnicos razoáveis disponíveis no momento do tratamento dos dados segundo Guidi (2018).

Dessa forma, os dados anônimos estariam fora do escopo de aplicação da lei, exceto se o processo de anonimato puder ser revertido ou se os dados forem usados para fins de criação de perfis comportamentais conforme ressaltou Soprana (2018). Efetivamente, dados anônimos são essenciais para tecnologias no âmbito da Internet das Coisas *(IOT)*[99], Inteligência Artificial (*AI*)[100], aprendizado de máquina, cidades inteligentes e análise de grandes contextos comportamentais.

Já os dados públicos continuando a abordagem de Soprana (2018), neste ponto tem havido muita discussão sobre os limites do uso de dados pessoais acessíveis ao público, como aqueles contidos em bancos de dados administrados por órgãos públicos, publicações oficiais e registros notariais, ou aqueles expressamente tornados públicos por seus titulares de dados, como perfis públicos em redes sociais.

Ainda vislumbrando a obra de Soprana (2018) a Lei Geral de Proteção de Dados (LGPD, 2018) lida com tais situações, tratando-as de maneiras diferentes e impondo certas limitações, como limitar o uso aos fins que levaram à divulgação dos dados pessoais acessíveis ao público. Isso não significa que os dados públicos não possam mais ser utilizados para outros fins, apenas que os modelos de negócios que contam com esse tipo de dados terão que se adaptar.

Logo chega-se aos fundamentos legais para o processamento de dados, consentimento e interesses legítimos, para qual o tratamento de dados pessoais, e o que inclui a prática de sua coleta, é sempre necessário ter uma base jurídica. A Lei Geral de Proteção de Dados (LGPD, 2018) enumera hipóteses que autorizam o uso de dados pessoais, e o consentimento inequívoco é apenas uma delas (Soprana, 2018).

Deve-se observar que a base jurídica conhecida como interesse legítimo, que não existia no quadro jurídico brasileiro anterior de proteção de dados, permitiria a utilização

---

[99] A Internet das Coisas (IoT) descreve a rede de objetos físicos, "coisas", que são incorporados a sensores, software e outras tecnologias com a finalidade de conectar e trocar dados com outros dispositivos e sistemas pela Internet. Esses dispositivos variam de objetos domésticos comuns a ferramentas industriais sofisticadas. Com mais de 7 bilhões de dispositivos IoT conectados hoje, os especialistas esperam que esse número cresça para 10 bilhões em 2020 e 22 bilhões em 2025. Recuperado em 06 de novembro de 2019, de https://www.oracle.com/internet-of-things/what-is-iot/.

[100] O Dicionário Oxford define Inteligência Artificial (IA) como a teoria e o desenvolvimento de sistemas computacionais capazes de realizar tarefas que normalmente requerem inteligência humana, como percepção visual, reconhecimento de fala, tomada de decisão e tradução entre idiomas. Recuperado em 05 de novembro de 2019, de https://www.lexology.com/library/detail.aspx?g=5424a424-c590-45f0-9e2a-ab05daff032d.

dos dados para fins diferentes daqueles originalmente autorizados por seus titulares de dados ou aqueles que os conduziram à sua divulgação como apontado por Pereira (2019). Por meio de um teste de proporcionalidade que leva em consideração os interesses dos controladores e os direitos do titular dos dados, essa hipótese permitiria novos usos para os dados, tornando-se imprescindível em tempos de '*Big Data'*, inteligência artificial, cidades inteligentes e da internet das coisas.

Nos princípios gerais de proteção de dados, a Lei Geral de Proteção de Dados (LGPD, 2018) enumera princípios que devem ser levados em consideração no tratamento de dados pessoais, como limitação da finalidade, necessidade, transparência, segurança, não discriminação e o novo princípio da responsabilidade, o que torna obrigatório que o responsável pelo tratamento e o processador de dados demonstrem de forma cabal e transparente a adoção de medidas efetivas capazes de comprovar o cumprimento das regras de segurança e proteção de dados sensíveis e pessoais. Isso pode ser feito por meio de avaliações de proteção de dados, e metodologias também previstas em lei (Soprana, 2018).

Também, de acordo com Fernandes (2018), quanto aos direitos básicos do titular dos dados, os titulares dos dados terão seus direitos básicos ampliados e deverão ser garantidos de forma acessível e efetiva, dentre os direitos elencados, é importante destacar o direito de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao tratamento, direito à informação e explicação sobre o uso dos dados.

A grande novidade é o direito à portabilidade dos dados, que permite ao titular dos dados não só solicitar uma cópia integral de seus dados, mas também tê-los disponibilizados em formato interoperável, que visa facilitar a sua transferência para outros serviços, mesmo para concorrentes (Soprana, 2018). Pela sua natureza, este novo direito tem sido visto como um forte elemento de competição entre diferentes empresas que oferecem serviços semelhantes baseados na utilização de dados pessoais.

Um dos principais pontos da Lei Geral de Proteção de Dados (LGPD, 2018) é a responsabilidade sobre os diferentes agentes envolvidos no processamento de dados, o controlador e o processador, que podem ser solidariamente responsáveis por incidentes de segurança da informação ou uso indevido e não autorizado dos dados ou por não conformidade com a lei (Fernandes, 2018).

No entanto, a responsabilidade do processador, ou seja, quem pratica o processamento de dados em nome do controlador, pode ser limitada às suas obrigações contratuais e de segurança da informação, se não violar as regras impostas pela Lei Geral de

Proteção de Dados (LGPD, 2018). Portanto, é importante definir se uma empresa deve ser vista como controladora ou processadora, ou ambos, para definir os limites de sua responsabilidade (Mendes & Mattiuzzo, 2019).

A notificação obrigatória de violação de dados para a autoridade de proteção de dados torna-se obrigatória e devem ser realizadas dentro de um prazo razoável, que pode, com base na gravidade do caso, determinar a notificação a todos os titulares de dados envolvidos e a ampla publicidade do incidente na linha do que observa Mendes & Mattiuzzo (2019).

No que diz respeito a transferências de dados internacionais a Lei Geral de Proteção de Dados (LGPD, 2018) brasileira traz uma série de instrumentos jurídicos que permitem a transferência internacional de dados pessoais, mesmo para países que não sejam considerados como tendo um nível de proteção adequado conforme ressalta Guidi (2018).

Será possível a transferência internacional de dados pessoais com base no consentimento específico e expresso do titular dos dados, que deve ser prévio e separado dos demais fins e requisições de consentimento. Também será possível efetuar a transferência se houver garantia, por parte do controlador, por meio de instrumentos contratuais, como regras societárias vinculativas e cláusulas padrão, de que cumprirá os princípios, direitos do titular dos dados e o regime de proteção de dados previstos na lei (Banisar, Guillemin, & Blanco, 2017).

Semelhante ao Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), a lei como observa Doneda (2019) permite a transferência por meio da adoção de selos, certificados e códigos de conduta emitidos e autorizados pela Autoridade de Proteção de Dados, como uma garantia notarial para a autenticidade de tais informações ou dados.

E o responsável pela proteção de dados será o ente regulador, aos moldes da UE, o *Data Protection Officer* (DPO), que será a pessoa singular, nomeada pelo responsável pelo tratamento, que atua como um canal de comunicação entre o responsável pelo tratamento, os titulares dos dados e a autoridade de proteção de dados (Soprana, 2018).

Além disso como observa Soprana (2018), o DPO deve ser responsável dentro da instituição pelo cumprimento pela empresa das normas previstas em lei e orientar os funcionários e contratados da entidade quanto às práticas a serem tomadas em relação à proteção de dados pessoais.

Uma primeira leitura da Lei Geral de Proteção de Dados (LGPD, 2018) permite concluir que qualquer entidade que trate dados pessoais deve indicar DPO, mas a autoridade de proteção de dados pode estabelecer normas complementares sobre a definição e as

atribuições do responsável, incluindo hipóteses sobre as quais as empresas não precisam nomear um *Data Protection Officer* (Soprana, 2018).

Quanto a avaliação de impacto na proteção de dados, ainda seguindo a pesquisa desenvolvida por Soprana (2018), é considerada em diversos pontos da legislação como um mecanismo de avaliação importante para verificar o impacto na proteção e segurança de dados pessoais e informações sensíveis, pois à documentação do controlador que contém a descrição das atividades de processamento de dados que podem criar riscos consideráveis para os titulares dos dados, bem como para as medidas, salvaguardas e mecanismos de mitigação implementados que buscam garantir a integridade das normativas de segurança.

O Relatório de Impacto à Proteção de Dados pode ser obrigatório em situações já caracterizadas como de risco ou, a requerimento da autoridade, quando o tratamento dos dados se baseia em legítimo interesse. A metodologia do Relatório de Impacto à Proteção de Dados é amplamente adotada pelo Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia e permite, além do mapeamento de riscos, uma fotografia efetiva da situação de conformidade regulatória da entidade (Banisar, Guillemin & Blanco, 2017).

Com isso o registro de atividades de processamento de dados passa por toda e qualquer atividade de processamento de dados e informações pessoais que deve ser registrada, desde a sua coleta até a sua exclusão, indicando quais os tipos de dados e informações pessoais que serão coletados, a base legal que autoriza seu uso, finalidades, tempo de retenção, as práticas de segurança da informação implementada no armazenamento e com quem os dados podem ser eventualmente compartilhados, metodologia esta conhecida como mapeamento de dados (Gellert, 2018).

Levando em conta as importâncias dos padrões de segurança da informação como apontado por Gellert (2018), o controlador de dados e o processador de dados devem tomar medidas técnicas, de segurança e administrativas adequadas para proteger os dados pessoais. A autoridade de proteção de dados pode estabelecer padrões técnicos mínimos, considerando a natureza dos dados tratados, as características específicas do seu tratamento e o estado atual da tecnologia que será utilizada.

A Privacidade, importante valor protegido pelas diversas legislações de dados ao redor do mundo, desde a concepção e por consequência das novas tecnologias, torna-se um item a ser obrigatório a adoptar desde a concepção dos serviços, produtos e modelos de negócio a prática de garantir os direitos de privacidade e proteção de dados e informações (Doneda, 2018).

Os princípios gerais da Lei Geral de Proteção de Dados (LGPD, 2018) e as normas de segurança devem, portanto, ser observados desde a concepção até a execução e oferta do produto e serviço, visto que apesar do constante aprimoramento das ferramentas legais para tornar juridicamente seguro e protegido o direito que diz respeito a dados e informações, é notório o também inegável a constante evolução de forma para burlar os sistemas de segurança ou as normas que garante a segurança e a proteção dos dados como bem observou a obra de Denardis (2014) em sua análise.

Além disso, os controles de privacidade, popularmente acessíveis por meio de painéis em plataformas *online*, devem, por padrão, ser os mais protetores e cabe aos titulares dos dados torná-los flexíveis conforme o caso, se assim o desejarem (Doneda, 2018).

Os códigos de conduta e organismos de certificação que estão a orbita do Lei Geral de Proteção de Dados (LGPD, 2018) são estimulados claramente a adoção de códigos de conduta da indústria e organismos de certificação que podem garantir a conformidade com as regras de proteção de dados (Soprana, 2018).

Certos setores da sociedade podem criar seus próprios códigos de conduta no uso e segurança de dados, que podem ser até superiores à Lei em alguns aspectos. Mas devem ser, como lembrando Santos (2018), previamente autorizados pela autoridade pública competente e fornece métodos que demonstrem conformidade com a norma jurídica vigente.

Além disso, as entidades podem habilitar-se perante a autoridade pública para certificar que outras instituições estão em conformidade com a lei geral, contudo isso também passar por diversos crivos que estão ligados as tecnicidades da norma legislativa e o entendimento das cortes de justiça (Santos, 2018).

Já as possíveis sanções que podem ser variadas, desde sanções administrativas que podem ser aplicadas pela autoridade pública em caso de violação da Lei Geral de Proteção de Dados (LGPD, 2018) dentre as sanções, estão autuações e multas, que podem variar de 2% do faturamento da empresa, grupo ou conglomerado no Brasil no último exercício social, limitadas no total de cinquenta milhões de reais por infração (Pinheiro, 2019). Também existe a possibilidade de uma multa diária para obrigar a entidade a cessar as infrações.

O período de transição e adaptação da Lei Geral de Proteção de Dados (LGPD, 2018) entrou em vigor 18 meses após sua publicação. Portanto, entidades públicas e privadas tiveram até fevereiro de 2020 para se adaptar. Além disso, a autoridade nacional, quando criada, pode estabelecer regras sobre a adaptação progressiva das bases de dados criadas até à data de entrada em vigor da Lei, tendo em conta a complexidade das operações de

tratamento e a natureza dos dados e informações que ali seriam tratadas e analisadas sob responsabilidade do poder público e do direito e das garantias constitucionais brasileiras. (Santos, 2018).

O Acordo de Processamento de Dados, ou em sua terminologia original, *Data Processing Agreement* (DPA), quando estabelecido, tornou-se de diversas formas a autoridade pública independente responsável pela supervisão da lei e da aplicação de sua proteção. Seu formato funciona da mesma forma que outras agências reguladoras ou fiscalizadoras (Pinheiro, 2019).

Em suma, de acordo com Pinheiro (2019), deve-se garantir a proteção dos dados e informações pessoais, conforme a Política Nacional de Proteção e Privacidade de Dados, de acordo com a lei, monitorar e aplicar sanções em caso de violação das leis pertinentes, atender às solicitações dos titulares dos dados contra os responsáveis pelo tratamento dos seus dados e às questões regulamentares em matéria de proteção de dados, entre outras atividades.

A Lei Geral de Proteção de Dados (LGPD, 2018) tem um impacto na sociedade como poucas leis tiveram antes, já que hoje praticamente todas as práticas da sociedade tratam do uso de dados e informações pessoais (Pinheiro, 2019). Empresas de todos os setores terão que se adaptar e se formar uma nova cultura sobre o uso adequado dos dados, algo difícil de se conseguir considerando que o Brasil, ao contrário de outras regiões do mundo, ainda está engatinhando no que diz respeito a este tópico.

Nesse sentido, seguindo o pensamento de Bassini (2019) a proteção de dados pessoais deve e pode ser vista não como um custo, mas como uma vantagem competitiva, um diferencial de mercado. Em uma época de grandes vazamentos de informações e escândalos sobre o uso indevido de dados, o cumprimento de regras claras, transparentes e harmoniosas pode restaurar ou aumentar a confiança do consumidor nas empresas e no mercado e do cidadão na administração pública.

Portanto, buscando observar os pontos da obra de Doneda (2019), as empresas e o estado precisam estar em conformidade com as regras de hoje e compreender que prever a regulamentação futura é um investimento e uma vantagem para toda a sociedade, e para seu modo de vida ao estar imersa e habituada a rotina do hoje, com sua constante evolução tecnológica e a imersão de um mundo globalizado de acesso à informação, assim como ter garantida a devida proteção de seus direitos no que diz respeito a suas informações privadas e sensíveis quanto a sua segurança e direitos e garantias constitucionais.

4. AS RELAÇÕES ENTRE GOVERNANÇA DIGITAL E ÉTICA DIGITAL COM A PROTEÇÃO DE DADOS

A sociedade da informação madura, não vive mais *online* ou *offline*, mas na vida, ou seja, vivemos cada vez mais naquele espaço especial, uma "infosfera"[101], que é perfeitamente analógico e digital, *offline* e *online* (Floridi, 2016). Nossas sociedades de informação maduras estão crescendo em um lugar novo, como resultado, o ritmo de sua evolução pode ser alucinante. E isso, por sua vez, justifica alguma apreensão.

No entanto, não devemos nos distrair com o escopo, profundidade e ritmo da inovação tecnológica. É verdade que isso rompe alguns pressupostos profundamente arraigados da sociedade analógica, seguindo a abordagem de Floridi (2016) por exemplo, sobre produção, logística, customização, educação, trabalho, saúde, entretenimento, política e segurança, apenas para mencionar alguns tópicos.

Sobre a governança do digital, há muito a ser dito, e mais ainda a ser compreendido e teorizado, mas um ponto é claro: a governança do digital, e a ética do digital, também conhecida como ética da informação ou dados (Floridi & Taddeo, 2016) e a regulação do espaço digital, que são abordagens normativas distintas, complementares, mas que não se confundem, são temas pertinentes ao direito constitucional de hoje.

Governança digital, seguindo o pensamento de Floridi (2016) tem se consolidado como a prática de estabelecer e implementar políticas, procedimentos e padrões para o desenvolvimento, uso e gerenciamento adequados do espaço *online* e *offline*.

É ainda uma questão de convenção e boa coordenação entre os pesquisadores do direito, pois em uma primeira avaliação podemos achar que nesta tese jurídica às vezes nem é moral nem imoral, nem legal nem ilegal, por meio da governança digital, onde uma agência governamental ou uma empresa pode determinar e controlar processos e métodos usados por administradores de dados e custodiantes de dados a fim de melhorar a qualidade dos dados, confiabilidade, acesso, segurança e disponibilidade de seus serviços e conceber procedimentos eficazes para a tomada de decisões e para a identificação de

[101] Infosfera é um neologismo criado pelo filósofo da informação Luciano Floridi, filósofo italiano conhecido pelo seu trabalho pioneiro no campo da Filosofia da Informação e da Ética da Informação, e que faz referência a um complexo ambiente informacional constituído por todas as entidades informacionais, suas propriedades, interações, processos e demais relações.

responsabilidades no que diz respeito aos processos relacionados com dados[102] e informações, que tinha como objetivo dar aos servidores orientações sobre a realização de projetos de informação de dados e a confiança para inovar com estes dados[103](Floridi & Taddeo, 2016).

A governança digital pode incluir diretrizes e recomendações que se sobrepõem, mas não são idênticas à regulamentação digital (Floridi, 2016). Esta é apenas mais uma forma de falar sobre as legislações pertinentes, em um sistema de regras elaborado e aplicado por meio de instituições sociais ou governamentais para regular o comportamento dos agentes relevantes na esfera administrativa dos espaços governamentais online além de seus bancos de dados que em sua maioria passam a ser totalmente digitais.

Nem todos os aspectos da regulamentação digital são uma questão de governança digital e nem todos os aspectos da governança digital são uma questão de regulamentação digital. Nesse caso, um bom exemplo é fornecido pelo Regulamento Geral de Proteção de Dados (RGPD, 2016), observado neste caso que a conformidade é a relação crucial por meio da qual a regulamentação digital molda a governança digital[104](Doneda, 2018).

Tudo isso vale para a ética digital, entendida como o ramo da ética que observa e avalia problemas morais relacionados a dados e informações, incluindo geração, registro, curadoria, processamento, disseminação, compartilhamento e uso de dados dos cidadãos, algoritmos que incluem Inteligências Artificiais, agentes artificiais, aprendizado de máquina e robôs além de práticas e infraestruturas correspondentes incluindo inovação responsável por programações, *hacking*[105], códigos e padrões profissionais do funcionalismo público, a fim de formular e apoiar soluções moralmente adequadas como a boa conduta ou bons

---

[102] Gabinete do Governo, Serviço Digital do Governo. (2016). Estrutura ética da ciência de dados. Recuperado em 25 de outubro de 2020, de https://www.gov.uk/government/publications/data-science-ethical-framework.

[103] Recuperado em 29 de outubro de 2020, de https://www.gov.uk/government/publications/data-science-ethical-framework.

[104] 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 de Proteção de Dados), OJEU L119, 04/05/2016.

[105] Hacking é a aplicação de tecnologia ou o conhecimento técnico para suplantar algum tipo de problema ou obstáculo. Recuperado em 18 de novembro de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/hacking.

valores institucionais e democráticos (Doneda, 2019). Neste ponto a ética digital molda a regulação digital e a governança digital por meio da relação de sua avaliação moral.

Logo as influencias dos valores jurídicos encontram as tendencias de inovações junto as ondas do governo eletrônico, que estão aumentando por meio de organizações públicas e no âmbito da administração dos estados em todo o mundo segundo Floridi (2016). Diversos governos estão usando informações e tecnologia de comunicação especialmente Internet ou rede baseada na *web*[106], para fornecer serviços entre agências governamentais e cidadãos, empresas, funcionários e outras agências não governamentais.

4.1 O modelo da governança digital no estado democrático de direito

A governança digital está além do escopo de um "*E-Government*"[107] segundo o trabalho de Harris (2000). Enquanto o governo eletrônico é definido como uma mera entrega do governo de serviços e informações ao público usando meios eletrônicos, a governança eletrônica permite participação direta do cidadão, dos constituintes e do estado em atividades políticas que vão além do governo e inclui também as novas tendencias originadas pelas inovações tecnológicas em uma "*e-Democracy*"[108], terminologia está, derivada em paridade do "E-*Government*", que consiste em participar de atividades políticas e do exercício dos direitos constitucionais fundamentais de forma online.

Em sua análise, Harris (2000) resume a governança eletrônica da seguinte forma, sendo a governança eletrônica, que não envolve apenas o site do governo e o *e-mail*. Não se

[106] Web consiste em um sistema para encontrar informações na internet, no qual documentos são conectados a outros documentos. Recuperado em 18 de novembro de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/web.

[107] Governo eletrônico, ou E-Government, consiste no uso das tecnologias da informação, além do conhecimento nos processos internos de governo e na entrega dos produtos e serviços do Estado tanto aos cidadãos como à indústria, e no uso de ferramentas eletrônicas e tecnologia da informação para aproximar governo e cidadãos. Recuperado em 21 de novembro de 2019, de https://publicadministration.un.org/egovkb/en-us/about/unegovdd-framework.

[108] E-democracia é uma combinação das palavras eletrônico e democracia, também conhecida como democracia digital ou democracia na Internet, é o uso de tecnologias de informação e comunicação (TIC) em processos políticos e de governança. Recuperado em 25 de novembro de 2019, de https://www.infopedia.pt/dicionarios/lingua-portuguesa/e-democracy.

trata apenas da prestação de serviços pela Internet. Não se trata apenas de acesso digital a informações governamentais ou pagamentos eletrônicos. Isso buscar mudar a forma como os cidadãos se relacionam com os governos, tanto quanto muda a forma como os cidadãos se relacionam entre si. Trará novos conceitos de cidadania, tanto em termos de necessidades, como de responsabilidades.

A governança eletrônica, por sua vez, permitirá que os cidadãos se comuniquem com o governo, participem da formulação de políticas públicas e que os cidadãos se comuniquem entre si e participem do processo político democrático. Portanto, no sentido mais amplo, o governo eletrônico tem mais implicações do que a governança eletrônica (Floridi 2016).

Compreender a concepção de Governo Digital que encapsula uma agenda mais ampla de renovação pode ser mais útil para distinguir esses dois conceitos diferentes, mas relacionados entre si. O governo eletrônico se refere ao uso por agências governamentais de tecnologias da informação, como redes baseadas na *web*, a Internet e a computação móvel, que têm a capacidade de transformar as relações com os cidadãos, empresas e outros ramos do governo (Harris, 2000).

Essas tecnologias como observa Doneda (2019) podem servir a uma variedade de fins diferentes, como a melhor prestação de serviços governamentais aos cidadãos, melhores interações com empresas e indústrias, capacitação dos cidadãos por meio do acesso à informação ou gestão governamental mais eficiente. Os benefícios resultantes podem ser inclusive a diminuição de corrupção dos agentes públicos, maior transparência, maior conveniência, aumento da receita nacional e redução de custos da máquina pública.

Algumas questões administrativas, políticas e éticas derivadas do governo eletrônico devem ser abordadas, como segurança, privacidade e exclusão digital. As implementações do governo eletrônico devem levar em consideração a segurança e a privacidade para garantir que os sistemas de informação e acervos sejam protegidos de forma adequada e os direitos individuais e garantias constitucionais sejam respeitados (Doneda, 2019). A segurança geralmente se refere à proteção dos ativos dos sistemas de informação e ao controle do acesso às próprias informações.

A aplicação da segurança seguindo o estudo de Doneda (2018) é específica para a situação e a sensibilidade das informações. Por exemplo, a proteção de segurança para informações públicas, como as atas das reuniões do conselho na *web*, não é rigorosa como seriam as informações específicas de um indivíduo, algo que deve chamar atenção de uma administração pública responsável, que deve olhar para o coletivo, mas para o privado.

Privacidade geralmente se refere ao respeito ao direito de que as informações atribuídas a um indivíduo sejam tratadas com um nível apropriado de proteção e segurança, assim como se espera de documento e informações de questões relacionadas à segurança ou administração de um país.

As leis de proteção à privacidade das informações costumam ser postas em prática para regular isso. Outro problema segundo Doneda (2019) é a divisão digital. Ao mesmo tempo, já foram expressas preocupações sobre a lacuna entre quem tem e não tem tecnologia e, mais popularmente, conhecido como "exclusão digital"[109], visto a disparidade entre diversos países em termos de infraestrutura, perícia técnica para a implementação dessa nova modalidade de governo, assim como a estabilidade política para fornecer segurança a todo o sistema de governo.

A fim de garantir que os países evitem criar uma exclusão digital, e criem condições para garantir que o crescimento da economia, do conhecimento, da garantia dos direitos constitucionais fundamentais, e assim vir a contribuir para a realização de um processo democrático de desenvolvimento eficiente, equitativo e sustentável, o diálogo ampliado e novos padrões de cooperação entre os setores público, privado e civil junto a organizações da sociedade são necessárias (Doneda, 2018).

O movimento para o governo eletrônico, em sua essência, está mudando a maneira como as pessoas e as empresas interagem com o governo (Floridi 2016). O governo eletrônico oferece um enorme potencial na busca de formas inovadoras de alcançar o ideal de governo das pessoas, pelas pessoas e para as pessoas. Esta pesquisa fornece apenas uma visão básica das diretrizes e estruturas que tratam da definição, características e tipos do governo eletrônico. Também impulsiona os recursos que permitem o planejamento, *design* e implementação do governo eletrônico por meio da revisão das iniciativas do governo eletrônico em todo o mundo (Doneda, 2018).

Ao analisar conceitos e referenciais teóricas nessas questões pode-se dar o contexto mais amplo abordado por Harris (2000) de iniciativas estruturais para o desenvolvimento do governo eletrônico e as recomendações para estudos futuros da governança digital na

[109] Exclusão digital e a desigualdade digital é um conceito dos campos teóricos da comunicação, sociologia, tecnologia da informação. e outras humanidades, que diz respeito às extensas camadas das sociedades que ficaram à margem do fenômeno das redes digitais. Contraste-se este conceito, por oposição, com a desigualdade digital. Recuperado em 22 de novembro de 2019, de https://news.un.org/pt/audio/2012/11/1047051.

administração pública. As questões de administração pública levantadas pelo governo eletrônico, como interface administrativa, administração digital e organização virtual, precisam ser analisadas sistematicamente e mais estudadas, especialmente na era digital que estamos inseridos e dependentes de diversas tecnologias. A Administração Pública no século XXI será em um mundo eletrônico, digital e virtual para os acadêmicos e profissionais da área, em especial um desafia para as ciências jurídicas que precisaram encontrar harmonia em seus dogmas e a sua hermenêutica jurídica (Harris, 2000).

4.2 Redesenhando a organização administrativa no estado de direito constitucional

A governança digital frente ao ritmo extraordinário das mudanças da área tecnológica e da inserção digital, onde o próprio termo "*eGovernment"*[110] é um tanto novo e, essencialmente, implica a atualização da eficiência e eficácia da máquina administrativa através da combinação de tecnologia da informação e multimídia sofisticada para entregar melhor, econômica e rapidamente serviços aos cidadãos (Harris, 2000). A Administração Pública está, de fato, em meio a um dos períodos de mudança mais rápida da história, onde os valores e garantia constitucional que só encontravam forma na letra da lei, ganha esse novo contorno diante da administração do estado em formato digital.

Assim, fatores como idade, analfabetismo e pobreza tornam-se barreiras para a receptividade das tecnologias digitais, barreiras que devem ser consideradas para garantir o acesso a todos de forma equânime aos direitos fundamentais garantidos em uma carta constitucional e consolidados em regimes democráticos de diversos países (Doneda, 2018).

A menos e até que essa barreira de conhecimento seja eliminada, há um risco significativo de que aqueles que mais precisam dos serviços se tornem os menos capazes de acessá-los em um novo mundo de discriminação tecnológica, ponto esse que deve ser observado pois estamos tratando de direitos fundamentais do cidadão como pertinentemente alerta a obra de Milakovich (2012).

[110]Países europeus apresentam iniciativas de governo eletrônico, principalmente relacionadas com a melhoria da governação a nível nacional. Atividades significativas de governo eletrônico também ocorrem a nível da Comissão Europeia. Recuperado em 16 de maio de 2020, de https://digital-strategy.ec.europa.eu/en/policies/egovernment.

As tendências emergentes da globalização e a abertura da Internet reúnem elites de todo o mundo em atividades organizadas como é apontado na obra de Doneda (2019). O surgimento de elites globais que controlam quase metade da riqueza do mundo diminui o potencial de democratização dos processos políticos que ensejam na modernização e democratização do acesso à informação e conhecimento (Hindman, 2009). Além disso, diferentes linguagens, sistemas de valores e consciência desigual da importância das tecnologias digitais podem impedir ainda mais o progresso humano e jurídico nesta área tão importante que deve ter espaço para crescer e ser democratizada universalmente.

As organizações que estão se convertendo para o modelo de governança digital devem levar em consideração a diversidade cultural conforme aborda Hindman (2009). O desenvolvimento de uma plataforma comum equipada com uma linguagem uniforme para interação, esclarecendo as culturas organizacionais e acomodando as diferenças, aumenta a probabilidade de as organizações reduzirem as brechas digitais resultantes da pobreza e da diversidade cultural (Doneda, 2018).

Estratégias colaborativas entre diversos órgãos públicos e a sociedade são vitais para uma mudança bem-sucedida de estratégias encaminhadas para a eficiência de um estado constitucional moderno que busca táticas orientadas para a democratização do acesso a proteção de dados de acordo com o pensamento de Doneda (2019).

Estas estratégias de gestão de desempenho podem e devem ser usadas para reforçar os valores essenciais de atuação no âmbito da gestão de um estado constitucionalista como por exemplo a redução de custos, eficiência, medição de resultados, satisfação de setores da sociedade e trabalho em esfera pública, além de claro e fazer os ajustes de fluxograma necessários para a melhor resposta possível na busca de garantir a ordem pública e garantir os direitos fundamentais assegurados a todos os cidadãos (Milakovich & Gordon, 2013).

Os governos geralmente ficam para trás em relação ao setor privado na gestão de desempenho como bem lembra Bioni (2019) porque contam com indicadores defasados e centros de coleta de dados obsoletos para avaliar o desempenho das suas agências e autarquias públicas. Para ajudar a melhorar a eficácia do agente público, os gestores públicos eleitos precisam de dados exatos, fidedignos e em tempo real.

Observando que os governos em todos os níveis precisam confiar mais na revisão contínua de dados, o que lhes permite perceber os problemas imediatamente e tomar ações a tempo para evitar que se tornem dificuldades incontroláveis, isso engloba dados desde meteorológicos para prevenção de catástrofes e a manutenção do bem estar social indo até a

segurança interna na busca constante da manutenção da ordem pública em um mundo cada vez mais globalizado, até mesmo no que diz respeito ao crime organizado, que ameaçam diretamente o direito fundamental da garantia a vida e segurança (Denardis, 2014).

No entanto, poucos administradores públicos, e cada vez menos funcionários eleitos, têm a consciência da importância de levar a habilidades estatísticas para o âmbito do direto na busca por uma maior segurança jurídica, necessária para utilizar plenamente as informações disponíveis em megabancos de dados baseados em "*nuvem"* em expansão como apontou Bioni (2019).

Logo é dever do estado implementar o processamento adicional que é necessário para a coleta e análise de dados avançados, pois esse é um caminho que se abre nas novas vertentes da manifestação do direito público em democracias cada vez mais envoltas as novas tendencias globalistas e tecnológicas (Viellechner, 2019).

Organizações públicas de todos os tipos podem ficar sobrecarregadas com a grande quantidade de diferentes tipos de dados e informações que requerem processamento em tempo real. Eles precisam desenvolver a capacidade de analisar mais e diferentes tipos de dados para aproveitar as vantagens das oportunidades ofertadas as democracias do mundo pelo "*Big Data"*. Além disso, conforme observa o pensamento de Tene & Polonetsky (2013) a oportunidade de processar fontes não estruturadas também é um fator importante nestes novos tempos da administração pública.

Lidar com megadados de forma eficaz requer a realização de mineração de dados em tempo real, e não depois de coletados e armazenados (Milakovich, 2012). Isso pode exigir a sensibilidade do poder público em buscar de especialistas externos, especialistas em concentrar vários pontos de dados em análises passíveis de decisão do interesse do estado.

A colaboração com o setor privado também é mais comum, com as empresas, entrando em uma miríade de novos acondicionamentos, contratos, parcerias e acordos cooperativos com fornecedores no qual os riscos e recompensas são compartilhados e o foco de ambas as partes é, ou espera-se que seja, menos no partidarismo e de ideologias políticas do que na entrega de melhores resultados aos membros da sociedade, na busca da maior excelência possível na modalidade das parcerias público-privadas (Bioni, 2019).

Ao contrário dos modelos de terceirização do passado, as estratégias de governança digital são projetadas conforme Bioni (2019) para alcançar parcerias colaborativas genuínas que vão além da mera instalação de tecnologia da informação, em vez disso, abrangem todas

as atividades necessárias para fornecer os ativos e serviços necessários do estado, levando a uma interação mais consistente e participativa entre estado e o cidadão.

Nos novos modelos de governança, esforços como esses são frequentemente vistos como intervenções de crise, em vez de estratégias de gestão de desempenho colaborativas abrangentes. Bretschneider (1990) explica em parte por que cultivar parcerias colaborativas genuínas é um desafio para o governo, pois a autoridade da organização pública deriva em parte de arranjos legais e constitucionais embutidos em freios e contrapesos tradicionais que causam maior interdependência além das fronteiras organizacionais (Gellert, 2018). Uma maior interdependência leva a níveis mais altos de supervisão, em vez de colaboração.

Além disso, um relacionamento mais cooperativo entre as entidades empresariais resulta do fato de que as empresas privadas são movidas pelo objetivo geral de maximizar os lucros. As organizações públicas não são voltadas para o lucro e frequentemente têm objetivos organizacionais múltiplos, políticos, complexos e, às vezes, concorrentes ou conflitantes como lembra Floridi (2016).

Essa diferença pronunciada entre os setores público e privado também torna mais difícil iniciar, organizar e aplicar projetos de uma cidadania digital inteligente em toda a esfera do estado constitucional (Thomas & Jajodia, 2004).

Apesar dos numerosos esforços para melhorar a comunicação e a colaboração entre os governos em todos os níveis como lembrado pro Gillespie (2017), as agências públicas têm contado principalmente com fontes únicas de dados que não são mais suficientes para lidar com os problemas cada vez mais complicados.

As ligações entre diferentes conjuntos de dados estão ocorrendo e continuarão no futuro. Isso ajuda a aumentar a interoperabilidade entre agências em diferentes níveis de governo e de entes privados (Black, 2012).

O compartilhamento eletrônico de dados entre as agências é aprimorado nos dias atuais em nome da prevenção do contraterrorismo e da proteção da segurança interna como aponta a obra da lavra de Viellechner (2019), que apesar de pontos políticos sensíveis de determinadas políticas internas, as lições aprendidas com esses aplicativos digitais em constante evolução está sendo transferidas para outras funções governamentais.

Contudo, observasse com contentamento que vários estados e governos locais atinando para o pensamento Thomas & Jajodia (2004) buscaram converter os sistemas tradicionais centrados na burocracia em uma governança em rede mais recente, centrada no cidadão, aprimorada pela "*nuvem"* em busca de agilidade e eficiência para dar um maior

acesso aos membros da sociedade ao sistema digital como um direito constitucional fundamental do ordenamento jurídico vigente.

4.3 A proteção de direitos fundamentais e seus riscos na esfera governamental da proteção de dados

A realidade fática da legislação que concebia o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) parte do pressuposto de que o processamento de dados pessoais é uma atividade arriscada. Em termos mais gerais, podemos associar a noção de gerenciamento de risco a toda tentativa adaptativa de reduzir a complexidade do ambiente humano. Do ponto de vista institucional, a atenção se deslocou das questões de gestão de risco para a rede de competências e instituições resumida na ideia de governança de risco (Milakovich, 2012).

As opções regulatórias de governança de risco dizem respeito a formas de autorregulação e suas variantes; ferramentas de regulação de cima para baixo, como atos, estatutos ou códigos aplicáveis, além de restrições administrativas; e uma combinação de tais formas e ferramentas (Milakovich & Gordon, 2013). Novos desafios também estão surgindo na forma de novas tecnologias e modelos de negócios, serviços e sistemas, segundo as pesquisas de Padovani & Santaniello (2018) depende-se cada vez mais de análises, *'Big Data*', compartilhamento de dados, rastreamento, criação de perfil e inteligência artificial.

Os espaços e ambientes que são habitados pelo cidadão comum e pelos quais se percorrem, geram e coletam dados do comportamento humano, informações essas que se bem tratadas pode revelar muito obre a estrutura de segurança de um país ou sobre a sua estabilidade democrática como pertinentemente observou Proxxima (2018).

Os dispositivos que são vestidos e carregados, e são instalados nos domicílios, os canais de comunicação, sensores para transporte e as ruas percorridas geram cada vez mais dados. As estruturas de proteção de dados podem ter seus limites e novos regimes regulatórios podem precisar ser desenvolvidos para lidar com os novos sistemas emergentes com uso intensivo de dados em tempo real.

Notavelmente, utilizando o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) como um parâmetro para análise de acordo com Bioni (2019), adotou-se esta última opção regulatória, de acordo com a qual a legislação pública estabelece os princípios que devem ser seguidos pelos controladores de dados e os resultados aos quais eles devem

obedecer. Depende dos controladores de dados, no entanto, sobre como eles deveriam atingir tais fins. Essa forma de corregulação gira em torno do que o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) atribui ao "*princípio da responsabilidade*"[111].

Indiscutivelmente, o RGPD teve um impacto maior na governança nacional e internacional do que nos dados dos cidadãos ou nas práticas do setor. Países ao redor do mundo estão agora debatendo ou aprovando uma nova legislação de privacidade, bem como entrando em ação com maior regulamentação contra os crescentes gigantes da tecnologia global. O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) é considerado um novo padrão, o qual muitos países aspiram se alinhar. Embora isso não signifique que o RGPD seja a meta regulatória final, ele apresentou uma meta ou marco para o qual outros países estão avançando, este é um posicionamento claro segundo Doneda (2019).

Em parte, essa abordagem reflete o vínculo da União Europeia entre a adoção de seus padrões de privacidade e seus acordos de livre comércio, por meio de decisões de adequação, visto que países como Nova Zelândia, Israel, Argentina, Japão, Colômbia, Coreia do Sul e Bermudas buscaram se espelhar padrões do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) em suas próprias reformas[112].

Ainda há muito trabalho a ser feito para garantir que a governança *online* seja legítima e justa. A experiência limitada do *Facebook* com as eleições americanas refletiu uma preocupação inicial sobre a governança de nossos espaços sociais *online* compartilhados. Infelizmente, o *Facebook* tratou esse processo como um fracasso e nunca tentou novamente experimentar para desenvolver um mecanismo melhor para buscar a

---

[111] O princípio da responsabilidade é mencionado apenas duas vezes no texto jurídico. O Recit. 85 do GDPR refere-se à responsabilidade em relação à responsabilidade por violações de dados e aos riscos para os direitos e liberdades dos titulares dos dados. O artigo 5.º, n.º 2, menciona o princípio como a forma através da qual os responsáveis pelo tratamento de dados podem provar o cumprimento dos «princípios relativos ao tratamento de dados pessoais» nos termos do art. 5 (1).

[112] A Comissão Europeia tem o poder de determinar, com base no artigo 45.º do Regulamento (UE) 2016/679, se um país fora da UE oferece um nível aceitável de políticas e legislações para a proteção de dados; 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 de proteção de dados) de 04/05/2016, p. 1–88; Recuperado em 02 de dezembro de 2020, de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R067.

opinião do usuário e consenso sobre seus processos de governança como fica evidente nos estudos de Foxx (2018).

Mas, como os princípios básicos de proteção de dados consagrados no Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) estão sendo concretizados na prática, um sistema fragmentado de governança de dados ainda é evidente. Embora o objetivo explícito da estrutura fosse a unificação de legislações existentes díspares, a incorporação do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679 na legislação nacional e a criação de agências para executá-lo não aconteceu de maneira uniforme em toda a Europa. Uma harmonia global sobre proteção de dados e privacidade é um ponto jurídico de extrema complexidade, mas vem se expandindo, e o impacto em países fora da União Europeia é evidente. Isso é verdade tanto dentro da Europa, em que se cita Suíça, Noruega, Islândia, Liechtenstein e fora, a própria Lei de Privacidade do Consumidor da Califórnia, a Lei de Proteção de Dados Pessoais da Índia e a atualização da Coreia do Sul da Lei de Proteção de Informações Pessoais estão entre os destaques globalmente[113].

Com essa compreensão dos direitos fundamentais em uma relação com a ênfase articulada no "risco" e nas técnicas de gerenciamento de risco introduzidas pelo RGPD (2016) como parte das obrigações de "responsabilidade" impostas aos controladores de dados para demonstrar conformidade. Essa constante "baseada no risco" está diretamente vinculada à proteção dos direitos fundamentais (Bioni, 2019).

No entanto, a relação entre risco e direitos e garantias fundamentais é teorizada nos estudos de direitos constitucionais em geral, de maneira amplamente imêmore por estudiosos de governança regulatória, que tendem a perceber os direitos em termos estreitos, seja como restrições colaterais ou como objetivos substantivos do esforço regulatório, ou ainda como um veículo através do qual os atores privados podem reivindicar os objetivos políticos subjacentes de um regime constitucional regulatório (Gellert, 2018).

Dentro das metodologias convencionais de avaliação de risco que se baseiam fortemente em uma família de métodos para o cálculo do risco com base nas ciências estatísticas, Gellert (2018) sugere que antes que qualquer cálculo de risco possa ser feito, é necessário primeiro identificar o evento indesejado ou adverso relevante. No entanto, em termos de governança regulatória, é feita uma distinção entre "*risco social*", ou seja, os riscos para a sociedade a partir de uma variedade de fontes, incluindo novas tecnologias, por um

[113] Lee A. Bygrave. (2014) 'Data Privacy Law: An International Perspective', Oxford University Press, 63.

lado, e "*risco institucional*" do outro, isto é, riscos para uma específica instituição decorrente de uma determinada atividade ou evento, os quais devem ser avaliados por agências regulatórias que desejam desenvolver e implementar "regulamentação baseada em risco" (Gellert, 2018).

No entanto, nem o conceito de "*risco à privacidade*" nem o de "*dano*" ocupam um lugar fundamental no texto do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016). Gellert (2018) aponta o fato na redação do Artigo 35 (1)[114] ao se referir ao "risco para os direitos e liberdades das pessoas físicas", por um lado, mas exigindo, se esse risco for alto uma avaliação do "impacto" sobre a proteção de dados pessoais e, assim, procura identificar o que a avaliação do Artigo 35 (1) realmente exige em termos de atenção ao cumprimento do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) ou os riscos que o processamento proposto representa para os direitos fundamentais (Gellert, 2018).

Isso indica, conforme Gellert (2018), que deve ser feita uma avaliação da natureza e magnitude das ameaças potenciais representadas pelo tratamento de dados pessoais aos direitos e liberdades das pessoas físicas, e que não precisam soar como danos tangíveis. Isso requer uma avaliação ampla da possível gama de interferências aos direitos fundamentais e constitucionais das pessoas físicas em geral, independentemente de seus dados pessoais serem ou não objeto do tratamento de dados proposto[115].

Entender o conceito de "risco aos direitos e liberdades das pessoas físicas" à luz do lugar dos direitos fundamentais no Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) e da natureza jurisprudencial dos próprios direitos constitucionais além de considerar como isso pode ser conciliado com uma abordagem "baseada em risco" para a segurança e proteção de dados e de informações (Gellert, 2018).

---

[114] Regulamento Geral sobre a Proteção de Dados (2016). CAPÍTULO IV. Responsável pelo tratamento e subcontratante; Artigo 35.. Avaliação de impacto sobre a proteção de dados; 1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.

[115] Artigo 35 (7) (b) do RGPD, que estabelece que a avaliação exigida nos termos do Artigo 35 (1) deve incluir medidas previstas para abordar os riscos, levando em consideração os direitos e interesses legítimos dos titulares dos dados e outras pessoas.

Para este efeito, a noção de "risco" e os "portadores de risco" relevantes adotados no regime europeu de proteção de dados em particular, são mais bem compreendidos à luz do Recit. nº 75 do RGPD[116], visto que o risco para os direitos e liberdades das pessoas singulares, de probabilidade e gravidade variáveis, pode resultar do processamento de dados pessoais que pode levar a danos físicos, materiais ou imateriais e ainda devemos observar o Recit. nº4 do RGPD[117] sobre a natureza do tratamento dos dados pessoais que deverá ser concebido para servir ao cidadão.

Conciliar essa tensão entre a linguagem e a compreensão do risco como construto estatístico, o discurso e a estrutura jurisprudencial dos direitos conforme apontam Gellert (2018) deve-se observar que o conceito do regime de "riscos aos direitos fundamentais", é o ponto que desencadeia a obrigação do Artigo 35 (1) do RGPD (2016) de realizar uma avaliação do impacto da proteção de dados. E pode ser melhor compreendido considerando

[116] Regulamento Geral sobre a Proteção de Dados (2016). Recit. (75) O risco para os direitos e liberdades das pessoas singulares, de probabilidade e gravidade variáveis, pode resultar do tratamento de dados pessoais, que pode levar a danos físicos, materiais ou imateriais, nomeadamente: quando o tratamento pode dar origem a discriminação , roubo ou fraude de identidade, perda financeira, danos à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional, reversão não autorizada de pseudonimização ou qualquer outra desvantagem econômica ou social significativa; nos casos em que os titulares dos dados possam ser privados dos seus direitos e liberdades ou impedidos de exercer controlo sobre os seus dados pessoais; onde os dados pessoais são processados que revelam origem racial ou étnica, opiniões políticas, religião ou crenças filosóficas, filiação sindical, e onde o tratamento de dados genéticos, dados relativos à saúde ou dados relativos à vida sexual ou condenações criminais e crimes ou medidas de segurança relacionadas; onde são avaliados aspectos pessoais, designadamente analisando ou prevendo aspectos relativos ao desempenho no trabalho, situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou movimentos, com vista à criação ou utilização de perfis pessoais; onde os dados pessoais de pessoas singulares vulneráveis, em particular de crianças, são tratados; ou quando o processamento envolve uma grande quantidade de dados pessoais e afeta um grande número de titulares dos dados.

[117] Regulamento Geral sobre a Proteção de Dados (2016). Recit (4) O tratamento de dados pessoais deve ser concebido para servir a humanidade. O direito à proteção de dados pessoais não é um direito absoluto; deve ser considerada em relação à sua função na sociedade e ser ponderada com os demais direitos fundamentais, de acordo com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, em particular o respeito pela vida privada e familiar, casa e comunicações, proteção de dados pessoais, liberdade de pensamento, consciência e religião, liberdade de expressão e informação, liberdade de conduzir negócios, direito a um recurso efetivo e a um julgamento justo e diversidade cultural, religiosa e linguística.

primeiro as práticas de processamento de dados propostas que apresentam uma violação clara dos fundamentos direitos, por exemplo, uma proposta para configurar assistentes domésticos inteligentes para que registrem e analisem continuamente todas as interações entre os ocupantes da casa para criar perfis detalhados de cada ocupante para fins de veiculação de publicidade direcionada (Bioni, 2019).

Em contraste, as operações de processamento propostas que poderiam ser consideradas limítrofes em que há alguma incerteza sobre se elas, se implementadas, constituem uma violação dos direitos fundamentais, talvez porque o tratamento proposto afeta os direitos fundamentais de uma forma nova ou porque pode ameaçar os "bens comuns" democráticos em que os direitos constitucionais estão ancorados podem cair no âmbito do Artigo 35 (1) do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) se a gravidade e a probabilidade da ameaça de risco aos direitos fundamentais são altas (Gellert, 2018).

Nesses casos limítrofes, Quelle (2017) indica em sua pesquisa que é prudente um maior nível de escrutínio, salvaguardas mais exigentes e apropriadamente uma maior cautela é garantida antes que tais práticas propostas possam prosseguir em nome da segurança do bom funcionamento do estado constitucional. Em uma apreciação das decisões dos tribunais e cortes europeias, que têm a palavra final ao fornecer uma interpretação autorizada dos requisitos do regime como aponta Quelle (2017), ressaltando que eles têm demonstrado consistentemente a importância de levar os direitos fundamentais a sério ao julgar disputas relativas a estas questões intimamente ligadas aos direitos e garantias constitucionais.

A incerteza associada ao significado das normas pode ser indesejável e onerosa no curto prazo, principalmente para entes regulares e atores privados regulados comprometidos com o cumprimento de suas normas (Gellert, 2018). No entanto, como ainda indica Quelle (2017) pode muito bem ser inestimável a longo prazo.

Dada a complexidade e sofisticação dos sistemas tecnológicos através dos quais os dados pessoais são processados e seus "*insights"* aplicados na prática contemporânea, e observando o compasso célere da inovação contínua em tecnologias baseadas em dados digitais, o foco no processamento de dados pessoais como o gatilho crítico para as disposições operacionais da organização da sociedade pode fornecer maior resiliência e durabilidade em face do avanço tecnológico (Quelle, 2017).

Assim entendida, a abordagem baseada em risco exigida pelo Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) exige que o controlador de dados realize uma

avaliação de risco de direitos fundamentais contextual, a fim de identificar o nível apropriado de rigor das medidas técnicas e organizacionais que devem ser adotadas para proteger contra esses riscos de se materializar, também conforme exigido pelos Artigos 24[118] e 25[119] do RGPD (2016), visto a análise feita no ambiente governamental (Quelle, 2017).

Além disso, a crise do COVID-19 tornou as questões de privacidade de dados ainda mais salientes. À medida que as organizações coletam informações pessoais sobre a saúde dos funcionários e viagens como parte de sua resposta para conter a propagação do vírus, elas precisam tomar medidas adequadas para proteger a privacidade dos funcionários e manter a conformidade com os regulamentos de privacidade de dados aplicáveis, incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia, a CCPA da Califórnia e a HIPAA dos Estados Unidos da América.

---

[118] Artigo 24. Regulamento Geral sobre a Proteção de Dados. 2016. Responsabilidade do responsável pelo tratamento; 1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades; 2 Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento; 3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.o ou de procedimentos de certificação aprovados conforme referido no artigo 42.o pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

[119] Artigo 25. Regulamento Geral sobre a Proteção de Dados. 2016. Proteção de dados desde a conceção 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; 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares; 3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.º 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.

Enquanto isso, hoje o risco de violar inadvertidamente essas regulamentações de privacidade de dados, porque suas medidas de segurança não estão acompanhando o cenário de riscos cibernéticos em constante evolução. As organizações são vulneráveis a uma variedade cada vez maior de esquemas de ataque cibernético de criminosos cibernéticos, hackers e terroristas cibernéticos patrocinados em alguns casos até por nações com objetivos obscuros como bem observou Soprana (2018). Essa abordagem neutra em termos de tecnologia evita selecionar tipos específicos de sistemas ou instrumentos tecnológicos que podem se tornar obsoletos rapidamente, pois por se tratar de organização social e defesa de valores e garantias constitucionais o estado deve estar preparado para ter a proficiência necessária para este novo momento que estamos vivendo como bem ressalta Celeste (2019).

Em outras palavras, lembrando a trilha estabelecida pela pesquisa de (Bioni, 2019), embora o nível atual de incerteza interpretativa e hermenêutica possa ser indesejável, essa abertura interpretativa pode ser necessária para tornar o contexto social atual à prova de futuro, de modo que seu significado e requisitos possam evoluir como a inovação tecnológica continua em sua marcha rápida para a frente de tipos específicos de sistemas ou instrumentos tecnológicos que podem afetar nossos direitos como membros de uma sociedade civilizada demonstrando o grande desafio de enfrentar as novas tendencias da interação dos seres humanos e as novas tecnologia arrebatadoras.

Mais de 120 países[120] já promulgaram leis de privacidade dessa natureza[121], pois cidadão, junto a governos estaduais e federais, observa Bioni (2019), iniciaram uma nova fase de como executar a administração pública em seus países e perceber a relevância de manter seus dados protegidos e garantir que isso com segurança, quando forem transferidos ou compartilhados, buscando de um estado constitucional que garanta a segurança de seu direito fundamental de proteção e segurança a dados e informações.

---

[120] À medida que mais e mais atividades sociais e econômicas acontecem on-line, a importância da privacidade e da proteção de dados é cada vez mais reconhecida. 128 de 194 países implementaram legislação para garantir a proteção de dados e privacidade. Igualmente preocupante é a coleta, uso e compartilhamento de informações pessoais a terceiros sem aviso prévio ou consentimento dos consumidores. A África e a Ásia mostram um nível semelhante de adoção, com 55 por cento dos países adotando tais legislações, dos quais 23 são países menos desenvolvidos. Recuperado em 03 de novembro de 2019, de https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[121] Greenleaf, Graham (2012). "Global Data Privacy Laws: 89 Countries, and Accelerating". Social Science Electronic Publishing, Inc. SSRN 2000034.

5. CONCLUSÃO

A aplicação do Regulamento Geral de Proteção de Dados (RGPD), em 2016, deu iniciou a uma grande mudança global para a privacidade dos dados, criando movimentos políticos que exigem mais direitos para os titulares dos dados, penalidades mais severas para as empresas e governos que coloquem em pratica novos regulamentos que acompanhem os avanços das tecnologias que, por vezes, ameaçam a segurança de informações e dos dados.

Com o aumento exponencial dos dados gerados pelo cidadão comum e, sobretudo, por grandes empresas, tornou-se vital que os órgãos governamentais tomem as medidas necessárias para proteger os direitos de seus cidadãos a segurança e o bom uso de seus dados.

Os regulamentos de proteção de dados garantem não apenas, a segurança dos dados pessoais dos indivíduos, como também regulam a coleta, o uso, a transferência e a divulgação dos referidos dados como aponta a obra de Doneda (2019). Estes regulamentos também fornecem acesso aos dados e informações dos indivíduos e impõem medidas de responsabilização para as organizações que processam dados pessoais e os complementam fornecendo soluções para o processamento não autorizado ou prejudicial.

O objetivo da proteção de informações e dados pessoais e sensíveis, como apontado por Soprana (2018) não é apenas proteger os dados pessoais, e sim tutelar os direitos e as liberdades fundamentais das pessoas que estão relacionados com esses dados e informações. Ao proteger os dados pessoais, é possível garantir que os direitos e liberdades das pessoas não sejam violados. Por exemplo, o processamento incorreto de dados pessoais, pode levar a uma situação em que uma pessoa é esquecida por uma oportunidade de trabalho ou, pior ainda, perde o emprego atual.

O não cumprimento dos regulamentos de proteção de dados pessoais pode levar a situações ainda mais penosas, em que é possível extrair todo o dinheiro da conta bancária de uma pessoa ou até mesmo causar uma situação de risco de vida pela manipulação de informações de saúde como também observou Soprana (2018).

Ressalta-se ainda que os regulamentos de proteção de dados são necessários para garantir um comércio e uma prestação de serviços justos e em favor do consumidor. Os regulamentos de proteção de dados pessoais causam uma situação em que, por exemplo, os dados pessoais não podem ser vendidos livremente, o que significa que as pessoas têm um maior controle sobre quem os faz ofertas e que tipo de ofertas fazem. O vazamento de dados

pessoais pode causar danos significativos à reputação das empresas e também penalidades, por isso é importante cumprir os regulamentos de proteção de dados pessoais.

Para garantir a segurança dos dados pessoais, é valido observar a pesquisa de Guidi (2018) e saber quais dados estão sendo processados, por que estão sendo processados e com que base. Além disso, é importante identificar quais medidas de proteção e segurança estão em uso. Tudo isso é possível por meio de uma auditoria minuciosa da proteção de dados, que identifica o fluxo de informações e se os regulamentos de proteção de dados estão sendo seguidos. A auditoria pode ser realizada respondendo a um conjunto de perguntas específicas que foram elaboradas para esse fim. Os resultados darão uma visão geral clara dos procedimentos e possíveis vazamentos de dados, que podem então ser interrompidos.

Existem duas razões principais pelas quais os governos devem buscar regulamentações abrangentes de proteção de dados, as leis precisam ser atualizadas para atender à realidade de hoje e que as pessoas têm compartilhado cada vez mais suas informações pessoais online e, de muitas maneiras, isso se tornou um 'mal necessário' se você pretende se comunicar nesta sociedade. Embora as regras de privacidade existam em muitos países e continuem sendo importantes para ajudarem a proteger as informações e os direitos fundamentais das pessoas, elas não foram adaptadas para atender aos desafios do mundo conectado de hoje.

As batalhas pela privacidade e proteção de dados já começaram. Poderosos grupos de interesses especiais, do *Google* ao *Facebook*, se reúnem em diversos congressos e casas legislativas pelo mundo para responder aos novos regulamentos de proteção de dados[122], e em especial de direitos, em um esforço para descartarem regulamentos semelhantes para proteger os membros de nossa sociedade. Parece que, embora as promessas de maior proteção contra esses grupos tenham sido feitas, a realidade é que o objetivo da indústria é manter o *status quo* dos dados como estão como demonstrou Doneda (2019).

Os dados são um ativo extremamente importante, e coletar e compartilhar dados pode ser um grande negócio na economia digital de hoje. Mas para uma empresa aproveitar as vantagens dos dados que está coletando com segurança e sucesso, ela precisa ter salvaguardas para garantir que os dados fiquem sob controle e os consumidores não estejam sujeitos a vigilância indesejada.

---

[122] Digital, Culture, Media and Sport Committee, "Disinformation and 'fake News': Final Report", the House of Commons to the United Kingdom, February 18, 2019, p.42 Recuperado em 03 de novembro de 2020, de https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

À medida que as empresas coletem quantidades crescentes de informações sobre seus clientes, esses clientes começam a ver as desvantagens potenciais dessa coleta de dados. A privacidade de dados é mais importante hoje do que nunca, e as empresas devem se preocupar muito com suas políticas e procedimentos de privacidade e segurança de dados por alguns motivos diferentes.

Neste momento, o cenário regulatório criou novas complicações para empresas de todos os tipos. Os regulamentos de privacidade de dados, como o California Consumer Privacy Act (CCPA, 2018) da Califórnia e o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016), da União Europeia afetaram significativamente a forma como as empresas podem coletar, armazenar e lidar com essas informações pessoais dos consumidores. Essas legislações são abrangentes e projetadas para fornecerem um nível de proteção legal aos membros da sociedade abrangidos que não estava disponível anteriormente conforme apontado por Gellert (2018).

De acordo com o Relatório de Defesa da Ameaça Cibernética da Imperva 2019, espera-se que 57,6% das organizações governamentais, 73,5% das organizações educacionais e 74,5% das organizações de varejo corram o risco direto de sofrer violações ou comprometimento de dados. Em 2019, constatou-se organizações como *Equifax, British Airways*, *Fortnite*, *Marriott Hotel Group* pagaram liquidações na casa dos milhões por violações de dados apontados nas pesquisas de Doneda (2019).

Como o setor público e em especial o setor privado observam, a obrigação de proteger os dados nunca foi tão grande. Não só precisa coletar, armazenar, processar e descartar dados de maneira compatível com as regulamentações, como também necessita ter políticas e práticas de segurança de informações sólidas que protejam os dados de seus clientes do uso mal-intencionado ou não autorizado.

A proteção da privacidade, das informações sensíveis e dos dados dos membros de nossa sociedade de forma integral na era moderna é essencial para uma governança democrática eficaz e adequada. No entanto, apesar do crescente reconhecimento e consciência do direito à privacidade e proteção de dados em todo o mundo, ainda faltam processos legais e institucionais e infraestrutura para apoiar a proteção de direitos corroborando o ponto de vista de Bioni (2019). Algumas partes do mundo, em particular, sofrem com um vazio: a falta de marcos regulatórios e legais em muitos países e a implementação e fiscalização deficientes em outros.

Como resultado, as inovações em políticas e tecnologias, práticas de dados do setor público e privado, são amplamente deixadas sem regulamentação e sem verificação, e isso terá implicações significativas para os direitos dos indivíduos, bem como para o desenvolvimento das economias e sociedades. Há também um desafio sistêmico e estrutural que vem agravando essa situação seguindo a senda demonstrada por Soprana (2018). Os processos de tomada de decisão e legislativos muitas vezes não estão sujeitos a nenhum ou apenas a um escrutínio público muito limitado.

Indiscutivelmente, o RGPD teve um impacto maior na governança nacional e internacional do que nos dados dos cidadãos ou nas práticas do setor. Países ao redor do mundo estão agora debatendo ou aprovando uma nova legislação de privacidade, bem como entrando em ação com maior regulamentação contra os crescentes gigantes da tecnologia global. O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) é considerado um novo padrão, o qual muitos países aspiram se alinhar. Embora isso não signifique que o RGPD seja a meta regulatória final, ele apresentou uma meta ou marco para o qual outros países estão avançando, este é um posicionamento claro segundo Doneda (2019).

O Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) é uma tentativa ambiciosa e pioneira de criar um padrão abrangente e unificado para privacidade digital e proteção de dados. Os problemas que abordam são complexos e, como mecanismo de aplicação, continuará a amadurecer com o tempo. No momento, seu mandato é basicamente educacional, exigindo transparência em nome de manter os cidadãos informados sobre o uso de seus dados. E tem tido muito sucesso em destacar práticas duvidosas com as quais apenas especialistas em tecnologia e acadêmicos estavam amplamente familiarizados antes de sua implementação. Em segundo lugar, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) pode ser uma ferramenta útil para policiar e conter os piores excessos e exploração como padrões obscuros, mineração de dados e assim por diante.

Uma harmonia global sobre proteção de dados e privacidade está se expandindo, e o impacto em países fora da União Europeia é evidente. Isso é verdade tanto dentro da Europa, em que se cita Suíça, Noruega, Islândia, Liechtenstein e fora, a própria Lei de Privacidade do Consumidor da Califórnia, a Lei de Proteção de Dados Pessoais da Índia e a atualização da Coreia do Sul da Lei de Proteção de Informações Pessoais estão entre os destaques globalmente[123].

[123] Lee A. Bygrave. (2014) ‘Data Privacy Law: An International Perspective’, Oxford University Press, 63.

As características mais comumente reproduzidas do Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) são provavelmente suas disposições sobre violações de dados, direitos do titular dos dados e responsabilidade. Sua abordagem de lei abrangente para proteção de dados em todos os setores e contextos também está se mostrando popular, à medida que os países se envolvem em atualizações generalizadas de suas leis para refletir os desafios colocados pela economia digital.

No entanto, é importante observar que, apesar de todas as suas virtudes, o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) pouco faz para questionar os modelos existentes. Os efeitos colaterais não intencionais emergentes são as consequências totalmente previsíveis de tratar os dados como uma mercadoria em vez de um bem coletivo; o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) certamente poderia aumentar o poder das grandes tecnologias ou reforçar as práticas de uso de dados preocupantes que inspiraram o RGPD para começar, pois parece que o RGPD falhou em mitigar o monopólio de fato que os gigantes da tecnologia têm na coleta e no uso de dados.

E, se é isso que precisa acontecer, é preciso mais do que o Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679. O controle burocrático nunca será tão eficaz quanto uma cidadania mobilizada e vigilante que usa vozes democráticas para exigir novas regras e uma sociedade diferente. Essa cidadania está começando a exigir, e merece, melhor governança de tecnologia, coleta de dados e tomada de decisão automatizada.

A importância do *'Big Data'* não é apenas resultado de seu tamanho ou da velocidade com que está crescendo cerca de 60% ao ano, mas também da realidade de que os dados vêm de uma incrível variedade de fontes. A Internet captura muitos dados. O *Facebook* sozinho tem mais de 800 milhões de usuários ativos, mais da metade dos quais se conectam todos os dias, que geram mais de 900 milhões de páginas da web e carregam mais de 250 milhões de fotos todos os dias segundo Santos (2018).

Em 2010, há muito tempo no tempo da Internet, os *sites* do *Google* eram usados por mais de 1 bilhão de visitantes únicos todos os meses, que gastavam 200 bilhões de minutos em seus sites. O *YouTube*, de propriedade do *Google*, ultrapassou 1 trilhão de reproduções

de vídeo em 2011. *E-mail*, mensagens instantâneas, chamadas *VOIP*[124] e outras comunicações geram dezenas de trilhões de mensagens gravadas todos os anos[125].

Cartões de crédito e débito, cheques e outras atividades financeiras fornecem um fluxo constante de bilhões de transações financeiras registradas todos os meses. E cada vez mais as redes de sensores de câmeras de vigilância por vídeo, computadores embutidos em automóveis, os mais de 15 bilhões de telefones celulares que carregamos, registram localizações, movimentos e atividades. Conforme Bioni (2019) pode-se falar de maneira significativa sobre a coleta onipresente de dados, em que quase tudo o que se faz resulta na captura e no armazenamento de dados por um ou mais terceiros.

Os governos também estão entre os maiores coletores e usuários de dados pessoais. Na verdade, o advento da nova revolução da informação já mostrou sinais de marcar um frenesi crescente entre as agências governamentais que desejam acesso extraordinário a informações para identificar transações de lavagem de dinheiro e financiamento do terrorismo, localizar suspeitos de crimes, identificar e bloquear pornografia infantil ou outra expressão regulamentada, aplicar leis de propriedade intelectual ou apenas aliviar a carga administrativa dos governos como observou Doneda (2019) em sua obra.

É significativo que esses dados sejam digitais. Eles podem ser armazenados, compartilhados, pesquisados, combinados e duplicados com velocidade extraordinária e a um custo muito baixo. E são acompanhados por *metadados*[126], dados sobre quando, onde e como as informações subjacentes foram geradas. Alguns especialistas estimam que pode haver cinco vezes mais *metadados* do que as informações que estamos cientes de criar, e esses *metadados* podem ser extraordinariamente reveladores.

---

[124] Segundo o Oxford Advanced American Dictionary, Voz sobre IP, também chamada de VoIP (Voice over Internet Protocol), telefonia IP, telefonia Internet, telefonia em banda larga ou voz sobre banda larga é o roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados. Recuperado em 09 de julho de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/voip.

[125] "Google and Facebook tighten grip on US digital ad market," eMarketer, 2017. Recuperado em 21 de dezembro de 2020, de https://www.emarketer.com/Article/Google-Facebook-Tighten-Grip-on-US-Digital-Ad-Market/1016494.

[126] Metadados, ou Metainformação, são dados sobre outros dados. Um item de um metadado pode dizer do que se trata aquele dado, geralmente uma informação inteligível por um computador. Os metadados facilitam o entendimento dos relacionamentos e a utilidade das informações dos dados. Recuperado em 11 de julho de 2019, de https://www.oxfordlearnersdictionaries.com/definition/english/metadata.

Ao pensar sobre a importância de *'Big Data'*, é fundamental lembrar conforme aborda Tene & Polonetsky (2013) que o acesso a tantos dados, de tantas fontes diferentes, e o poder de computação para processá-los, cada vez mais significa que se pode perceber padrões, envolver-se em descobertas, e descobrir segredos até então ocultos.

Esse poder recém-descoberto já rendeu sucessos fabulosos em campos, como a pesquisa médica, no qual as interações medicamentosas e a eficácia dos tratamentos podem ser avaliadas de maneiras nunca antes possíveis e sem colocar vidas em risco por meio da pesquisa de intervenção. Mas, segundo Proxxima (2018), a mesma capacidade demonstrou tornar a desidentificação mais difícil, como o *Google* e a *Netflix* descobriram ao disponibilizar conjuntos de dados anônimos para pesquisa.

Considere, por exemplo, o fascínio demonstrado pela diretiva de proteção de dados e o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016) da União Europeia proposto, de forma semelhante à lei na maior parte do resto do mundo, com aviso e escolha ou consentimento como ferramentas principais de proteção de dados. Apesar das evidências crescentes de que os indivíduos ignoram os avisos, muitas vezes não entendem as escolhas que não são significativas em qualquer caso e resistem a fazê-las, a menos que sejam obrigados a realizá-lo, nesse caso, quase sempre fazem a escolha necessária para obter o desejado serviço ou produto, e observa-se que os reguladores continuam a se apegar a esses conceitos. Mas, independentemente do sucesso do aviso e da escolha até o momento, como essas ferramentas se sairão em um mundo de vigilância onipresente, e milhares de trocas de dados por e sobre cada indivíduo no planeta todos os dias? Em pouco tempo, o maior banco de dados do planeta pode conter avisos de privacidade exigidos por lei que ninguém leu.

Mesmo quando os redatores legislativos demonstram consciência de que o processamento de dados em uma escala muito grande pode gerar preocupações específicas, podem faltar evidências de que as implicações práticas dos riscos são compreendidas. Por exemplo, o projeto de Regulamento Geral sobre a Proteção de Dados da União Europeia prevê uma exceção à proibição geral de transferências de dados pessoais para países que carecem de proteção adequada, quando uma transferência "não pode ser qualificada como frequente e massiva[127]. Embora o uso do termo “massivo” sugira uma apreciação do desafio

[127] Artigo 44 (1) do Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679, o Princípio geral das transferências; Qualquer transferência de dados pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas

do *'Big Data'*, nenhuma tentativa é feita para definir o conceito ou mesmo colocá-lo em um contexto relativo como bem aponta Balkin (2018).

O ambiente digital dos entes protegidos pelos valores constitucionais também colocará a segurança e proteção de dados e informações em um contexto diferente. Frequentemente fala-se sobre os dados serem a 'moeda' da era da informação, mas em um mundo no qual os dados representam indivíduos em mais e mais transações e fornecem a base para a tomada de decisões, questões como acessibilidade, precisão e confiabilidade dos dados podem importar tanto ou talvez mais do que privacidade.

Isso parece especialmente verdadeiro com a computação em nuvem. Assim como a segurança nacional tende a superar a privacidade na maioria dos programas antiterrorismo e de aplicação da lei, à medida como abordou Tene & Polonetsky (2013) que demonstra dados e aplicativos críticos sendo armazenados remotamente, e a acessibilidade pode se tornar mais importante do que a sua proteção ou privacidade em nome de ideologias de defesa de soberanias ou segurança de determinados países.

Talvez o maior impacto, seja a pressão que ele traz para um novo debate multinacional bem informado sobre os princípios-chave que devem embasar a proteção de dados e informações. A maioria das leis de proteção de dados continua a se basear nas Diretrizes da OCDE[128] de 1980 (Greenleaf, 2013). Essas diretrizes resistiram bem as três décadas intermediárias, mas é importante lembrar que elas foram criadas não apenas, mas também antes da própria democratização da internet, *laptops* portáteis, GPS, *smartphones*, *tablets* ou uma miríade de outras inovações que tornam possível a pluralização da informação e do acesso a ela.

Identificar princípios comuns para embasar as leis de proteção de dados é fundamental não apenas para harmonizar essas leis, mas também para garantir que sirvam a fins valiosos e apropriados. O direito constitucional no seu ambiente digital destaca a necessidade de focar não apenas em “o quê” e “como”, mas também em “por quê'.

---

pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.

[128] Organização para a Cooperação e Desenvolvimento Econômico (OCDE), organização econômica intergovernamental com 38 países membros, fundada em 1961 para estimular o progresso econômico e o comércio mundial.

Existem limites quanto ao que pode ser feito com informações precisas e obtidas legalmente? Eles se aplicam a todos, até mesmo para atividades de segurança nacional, antiterrorismo e de aplicação da lei e da garantia da ordem pública? O foco no uso assume uma nova importância à medida que as aplicações tecnológicas diminuem o papel da lei na regulamentação da coleta e do compartilhamento de uma diversidade de informações e dados disponíveis para a coleta quase que instantânea no ecossistema digital em que estamos imersos.

Deve continuar a haver um "princípio de limitação de coleta" em um mundo de dados onipresentes e uma disposição aparentemente insaciável do público em fornecer seus dados *online* e *offline*? A privacidade está envolvida se o governo ou uma empresa observar, mas não agir com base nos dados obtidos legalmente, por exemplo, ao comparar listas de passageiros com bancos de dados de suspeitos de terrorismo? Existe um papel adequado para o consentimento individual? Acredita-se que a resposta é claramente sim, mas determinar os contornos dessa função em um mundo de *'Big Data'* não está sendo fácil e aparentemente será uma missão hercúlia aos legisladores e estudiosos do constitucionalismo.

Como podemos equilibrar o esforço para fazer isso com compromissos nacionais compartilhados com a liberdade de expressão? Qual é o papel adequado e prático do governo diante de um dilúvio de informações e dados digitais? O grande volume de dados pessoais sugere que o governo deve estabelecer em lei os direitos e obrigações básicas, mas como eles devem ser cumpridos devido ao desequilíbrio de recursos? Como os governos ou reguladores independentes exercem uma supervisão significativa de mais de 60 bilhões de transações de cartão de crédito e débito, 90 trilhões de *e-mails*, 1,4 trilhão de pesquisas na Internet e um grande número de outras transferências de dados como foi evidenciado pelo Stanford Internet Observatory (2019)[129] que ocorrem todos os anos?

Um exemplo recente de uma abordagem ambiciosa para coleta de inteligência *online* é uma fórmula de interesse do Centro de Informações Estratégicas e Operações do *Federal*

[129] O Stanford Internet Observatory é um programa do Cyber Policy Center, baseado no Freeman Spogli Institute for International Studies , o principal instituto de pesquisa da Universidade Stanford para o estudo de assuntos internacionais. o Observatório é uma iniciativa interdisciplinar composta por pesquisa, ensino e engajamento de políticas que abordam o abuso das tecnologias de informação atuais, com um foco particular nas mídias sociais. Isso inclui a disseminação de desinformação, violações de segurança cibernética e propaganda terrorista. Recuperado em 14 de novembro de 2019, de https://cyber.fsi.stanford.edu/io.

Bureau of Investigations (FBI) dos Estados Unidos da América, o ('FBI SIOC')[130], em desenvolvem uma solução de aplicativo de alerta, mapeamento e análise de mídias sociais. Entre muitas outras coisas, além de e analisar seus movimentos, vulnerabilidades, limitações e possíveis ações adversas, aos moldes de um filme de ficção cientifica, o aplicativo pode permitir que o FBI reveja desenvolvimentos prováveis na situação ou futuras ações tomadas por infratores em potencial

Precisa-se repensar o conceito ou a aplicação da soberania nacional no contexto de fluxos de dados inerentemente globais? Como observou a Autoridade Europeia para a Proteção de Dados, embora a jurisdição do legislador comunitário se limite ao território da União Europeia, as fronteiras externas tornam-se menos relevantes para os fluxos de dados. A economia depende cada vez mais das redes globais. Em geral, o local físico de uma operação de processamento é o menos relevante[131].

Além disso, as leis de proteção de dados em vários países expõem princípios básicos amplamente semelhantes e compartilham muitos pontos em comum em termos de padrões de aplicação, observando o contexto democrático e constitucionalista, buscando segundo Bioni (2019) a preservação e a consolidação dos valores e direitos fundamentas dos estados democráticos constitucionais de direito.

Um resultado significativo e contribuidor para o desenvolvimento de *'Big Data'* é o quanto se depende de sistemas baseados em dados para decisões e aplicativos críticos. Não é exagero dizer que são nada mais do que uma coleção de dados para a maioria das instituições, e muitas das pessoas, com quem se lida. Não é simplesmente que as biografias são gravadas nos uns e zeros que se deixa para trás nas transações digitais diárias, como

---

[130] O Strategic Information and Operations (SIOC) ou Center Centro de Informações Estratégicas e Operações é o centro de comando e comunicações global do FBI que opera 24 horas por dia para buscar e fornecer informações estratégicas à liderança do FBI, coletando e processando informações em tempo real; Recuperado em 19 de março de 2020, de https://www.fbi.gov/services/cirg/sioc.

[131] Peter Hustinx, Parecer da Autoridade Europeia para a Proteção de Dados sobre a Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o seguimento do Programa de Trabalho para uma melhor implementação da Diretiva Proteção de Dados. Recuperado em 02 de abril de 2020, de http: //www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf.

escreveu a professora Kathleen Sullivan[132] da Faculdade de Direito de Stanford, é que são essas coleções de zeros e uns que identificam, descrever e cada vez mais definem uns para os outros.

O constitucionalismo na sua versão digital apresenta enormes desafios para a proteção de dados tanto por processadores quanto por reguladores. Simultaneamente, muda o contexto e aumenta as apostas para a proteção de informações e dados da sociedade como um todo seguindo a obra de Celeste (2019). Não é de surpreender que, dado o ritmo da mudança, haja poucas evidências de que a proteção desses dados e de informações estejam se mantendo.

Nada obstante, acredita-se que a ampla harmonização em nível global, ainda será um desafio extremo a ser vencido dentro do ordenamento jurídico de diversos países em um futuro próximo[133]. Este entrave é causado, em parte, por causa da força de diferenças ideológicas e culturas arraigadas em todo o mundo. O *'Big Data'* também aumenta a importância da harmonização, ou mesmo da padronização, nos padrões de segurança e proteção de dados. Como os dados pessoais são coletados e compartilhados universalmente através das fronteiras setoriais e nacionais, leis de proteção de dados inconsistentes representam ameaças crescentes para indivíduos, instituições e sociedade.

.

[132] Sullivan, KM. (2003). 'Under a watchful eye: incursions on personal privacy' in: Leon, R.C., & Anrig, G (orgs.). *The War on our freedoms: civil liberties in an age of terrorism* (The Century Foundation, Nova York. 128, 131.

[133] Reidenberg, JR. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, 52 Stan, 1315-1371.

REFERENCIAS

Abreu, J. S. (2018). Jurisdictional battles for digital evidence, MLAT reform, and the Brazilian experience. *Revista de Informação Legislativa: RIL*, *55*(220), 233–257. Recuperado em 01 de julho de 2019, de https://www12.senado.leg.br/ril/edicoes/55/220/rilv55n220p233.pdf.

Aieta, V. S. (2014). *Marco civil da internet: marco civil da internet e o direito à intimidade*. São Paulo: Atlas.

Balkin, J. M. (2004). Digital speech and democratic culture: a theory of freedom of expression for the information society. *New York University Law Review*, *79*(1), 1-5.

Balkin, J. M. (2018). *Free speech in the algorithmic society: big data, private governance, and new school speech regulation.* 1149–1210. University of California, Davis.

Banisar, D., Guillemin, G., & Blanco, M. (2017). *Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional.* Recuperado em 19 de outubro de 2019, de http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-deDados-Pessoais-no-Brasil-ARTIGO-19.pdf.

Barroso, L. R. (2014). *A dignidade da pessoa humana no direito constitucional contemporâneo – a construção de um conceito jurídico à luz da jurisprudência mundial.* Belo Horizonte: Fórum.

Bassini, M. (2019). Fundamental rights and private enforcement in the digital age. *European Law Journal*, *25*(2), 182–197.

Baur-Ahrens, A. (2017). The power of cyberspace centralisation: analysing the example of data territorialisation. *University Press Scholarship Online, 1*(17), 36-56.

Berman, P. S. (2005). Cyberspace and the state action debate: the cultural value of applying constitutional norms to "private" regulation. *University of Colorado Law Review, 71*(40), 1263-1310. Recuperado em 22 de outubro de 2019, de https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1083&context=faculty_publications.

Berman, P. S. (2007). *Law and society approaches to cyberspace.* Ashgate: Publishing.

Bermant, P. S. (2002). The globalization of jurisdiction. *University of Pennsylvania Law Review, 151,* 311. Recuperado em 26 de setembro de 2019, de https://scholarship.law.upenn.edu/penn_law_review/vol151/iss2/1.

Bessa, J. (2014). *O escândalo da espionagem no Brasil.* Brasília: Thesaurus.

Bioni, B. R., & Mendes, LS. (2019). O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. *Revista de Direito do Consumidor*, *124*(2), 157-180.

Bioni, B. R. (2019). *Proteção de dados pessoais: a função e os limites do consentimento.* Rio de Janeiro: Forense.

Black J. (2012) *Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis*. Modern Law Review 75(6), 1037–1063.

Bloch-Wehba, H. (2019). Global platform governance: private power in the shadow of the state. *SMU Law Review*, *72*(1), 27–80.

Böckenförde, E. W. (2017). Fundamental rights as constitutional principles. In: *Constitutional and political theory - selected writings*. 186–208. Oxford: Oxford University Press.

Brasil. *Constituição da República Federativa do Brasil, 1988.* Brasília: Senado Federal.

Brasil. *Lei n. 13.709 de 14 de ago. de 2018*. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Recuperado em 25 de agosto de 2020, de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm.

Brasil. *Lei n. 13.853 de 8 de jul. 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. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm. Acesso em: 25 ago. 2020.

Bretschneider, S. (1990). "Management Information Systems in Public and Private Organizations: An Empirical Test." Public Administration Review, 50.

British Academy, The Royal Society. (2017). Data management and use: governance in the 21st century—a joint report by the British Academy and the Royal Society.

Bygrave, L. A. (2014) 'Data Privacy Law: *An International Perspective'*, Oxford University Press, 63.

Cabral, R. (2020). A questão dos metadados tem sérias implicações para a privacidade. Recuperado em 04 de fevereiro de 2021, de http://revistagalileu.globo.com/Revista/Common/0,,EMI340880-17770,00-A+QUESTAO+DOS+METADADOS+TEM+SERIAS+IMPLICACOES+PARA+A+PRIVACIDADE.html.

Canaris, C. W. (1989). Grundrechtswirkungen und verhältnismässigkeitsprinzip in der richterlichen anwendung und fortbildung des privatsrechts. *JuS*, *1*(2), 161-172.

Carta dos Direitos Fundamentais da União Europeia 2000. (2012). Versão consolidada. *Jornal Oficial C.*, *326*, 391–407. Recuperado em 17 de agosto de 2019, de https://www.europarl.europa.eu/charter/pdf/text_pt.pdf.

Castro, C. S. E. (2005). Direito da Informática, privacidade e dados pessoais. Coimbra: Almedina.

Celeste, E. (2019). Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers and Technology*, *33*(1), 76–99.

Colombo, C., &, Facchini Neto, E. (2017). Ciberespaço e conteúdo ofensivo gerado por terceiros: a proteção dos direitos de personalidade e a responsabilização civil dos provedores de aplicação, à luz da jurisprudência do Superior Tribunal de Justiça. *Revista Brasileira de Políticas Públicas, 1*(3), 217–237.

Correia, J. A. (2018). *Direito Público: Luso-Brasileiro*. (1ª ed.). Coimbra, Portugal: Editora GestLegal.

Costa, M. da. (2003). A internet e sua regulação internacional. In: Campos, D.L. de., Martins, I.G.S. *O direito contemporâneo em Portugal e no Brasil*. 577-618. Coimbra: Almedina.

Crespo, D. L., & Ribeiro Filho, D. (2019). A evolução legislativa brasileira sobre a proteção de dados pessoais: a importância da promulgação da lei geral de proteção de dados pessoais. *Revista de Direito Privado, 20*(98), 161-186.

Dance, G. J. X., Confessore, N., & Laforgia, M. (2018). *Facebook gave device makers deep access to data on users and friends: the company formed datasharing partnerships with apple, samsung and dozens of other device makers, raising new concerns about its privacy protections.* Recuperado em 06 de janeiro de 2019, de https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partnersusers-friends-data.html.

DaskaL, J. (2019). Privacy and security across borders. *The Yale Law Journal*. Forum, *1029,* 1–16. Recuperado em 22 de janeiro de 2020, de https://www.yalelawjournal.org/forum/privacy-and-security-across-borders.

Degenhart, C. (2011). Verfassungsfragen der internet-kommunikation: wie die rundfunkfreiheit in die online-welt hineinstrah. *Computer und Recht,* p. 231–237.

DeHert & Gutwirth (2006). *Privacy, data protection and law enforcement*. Privacy and the Criminal Law. Ed. Oxford, UK.

Denardis, L. (2014). *The Global War For Internet Governance.* New Haven and London: Yale University Press.

Determann, L. (2018). *California Privacy Law – Practical Guide And Commentary U.S. Federal and California Law*. (3rd ed.). IAPP.

Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. (1995). Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial L., 281,* 31–50. Recuperado

em 05 de setembro de 2019, de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

Doneda, D. (2011). A Proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law*, *12*(2), 91-108. Recuperado em 11 de agosto de 2019, de http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315.

Doneda, D. (2006). *Da privacidade à proteção de dados pessoais.* Rio de Janeiro: Renovar.

Doneda, D. (2019). *Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados*. (2ª ed.). São Paulo: Thompson Reuters Brasil.

Doneda, D. (2018). *O que está em jogo com a nova Autoridade Nacional de Proteção de Dados.* Recuperado em 15 de setembro de 2019, de https://www.jota.info/opiniao-eanalise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-dedados-13082018.

Doneda, D., & Córdova, Y. (2017). *Um lugar para os robôs (nas eleições): A utilização de APIs para o controle das informações que circulam em redes de bots.* Recuperado em 19 de agosto de 2019, de https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes20112017.

Elias, P. S. (2017). *Algoritmos, Inteligência Artificial e o Direito*. Recuperado em 02 de abril de 2019, de https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf.

Elola, J. (2018). *O reconhecimento facial abre caminho para o pesadelo de George Orwell: Tecnologia ameaça a privacidade das pessoas e abre as portas à distopia descrita no livro '1984'. Por outro lado, permite identificar em tempo recorde terroristas logo após cometerem atentados.* Recuperado em 27 de outubro de 2019, dehttps://brasil.elpais.com/brasil/2018/01/05/tecnologia/1515156123_044505.html.

Espanha. *Ley Orgánica nº 15, de 13 de dezembro de 1999.* Boletín Oficial del Estado. Madri, 14 dez. 1999. p. 43088-43099.

Fernandes, V. O. (2018). *Regulação de Serviços de Internet: desafios da regulação de aplicações Over-The-Top (OTT).* Rio de Janeiro: Lumen Juris.

Ferreira, P. (2006). *A Protecção de Dados Pessoais na Sociedade de Comunicação: Dados de Tráfego, Dados de Localização e Testemunho de Conexão*. Lisboa: O Espírito das Leis Editora, Ltda.

Fetzer, T., Yoo, CS. (2012). New technologies and constitutional law. *Faculty Scholarship at Penn Law*, *13*, 23.

Floridi, L. (2016). Mature information societies—a matter of expectations. Philosophy & Technology, 29.

Floridi, L., & Taddeo, M. (2016). What is data ethics? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences.

Foxx, C. (2018). *Google e Facebook são acusados de violar nova lei de proteção de dados da Europa.* Recuperado em 07 de novembro de 2019, de https://www.bbc.com/portuguese/internacional44259419https://www.bbc.com/portuguese/internacional-44259419.

Francisco, D., & Francisco, S. (2019). *Regulamento Geral de Proteção de Dados: 7 passos para uma metodologia de implementação do RGPD na Administração Pública.* Lisboa: Edições Sílabo.

Gellert, R. (2018) *Understanding the Notion of Risk in the General Data Protection Regulation*. Computer Law and Security Review 34, 279–288.

Gill, L., Redeker, D., & Gasser, U. (2015). Towards digital constitutionalism? mapping attempts to craft an internet bill of rights. *Research Publication*, 15(9), 7641.

Gillespie, T. (2017). Governance of and by platforms. In Burgess, J., Poell, T., Marwick, A. (Eds.), SAGE *handbook of social media.* SAGE. Recuperado em 04 de fevereiro de 2019, de http://culturedigitally.org/2016/06/governance-of-and-by-platforms/.

Gonçalves, V.H.P. (2017). *Marco civil da internet comentado.* São Paulo: Atlas.

Greenleaf, G. (2012). "*Global Data Privacy Laws: 89 Countries, and Accelerating*". Social Science Electronic Publishing, Inc. SSRN 2000034.

Greenleaf, G. (2013). "*Modernising' data protection Convention 108: A safe basis for a global privacy treaty?*", Computer Law & Security Review, Vol. 29, 4.

Guidi, G.B.C. (2018). *Privacidade em perspectivas: modelos regulatórios para proteção de dados pessoais.* Branco, S., & Chiara de Teffé, C. (orgs.). Rio de Janeiro: Lumen Juris.

Gurses, S., Troncoso, C., & Diaz, C. (2015). *Engineering Privacy by Design.* Institute IM Idea. Recuperado em 08 de dezembro de 2019, de https://summerschool-croatia.cs.ru.nl/2017/slides/Engineering%20privacy%20by%20design.pdf.

Harris, B. (2000). *E-Governance.* Recuperado em 01 de março de 2019, de http://www.iadb.org.

Hindman, M. (2009). *The Myth of Digital Democracy.* Princeton, N. J.: Princeton University Press.

Itália. *Legge nº 675, de 31 de dezembro de 1996.* Gazzetta Ufficiale della Repubblica Italiana. Roma, 8 Jan. 1997.

Johnson, D.R., & Post, D. (1996). Law and borders - The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402.

Jóri, A. (2016). Protection of fundamental rights and the internet: a comparative appraisal of German and Central European constitutional case law. In: T*he Internet and Constitutional Law: The protection of fundamental rights and constitutional*

adjudication in Europe. Londres e Nova Iorque. Routledge Taylor and Francis Group.

Kerr, O. S. (2004). The fourth amendment and new technologies: constitutional myths and the case for caution. *Michigan Law Review, 102*, 801–888.

Krisch, N. (2010). *Beyond Constitutionalism: The Pluralist Structure of Postnational Law*. Oxford: Oxford University Press.

Ladeur, K. H., & Viellechner, L. (2008). Die transnationale Expansion staatlicher Grundrechte Zur Konstitutionalisierung globaler Privatrechtsreg. *Archiv des Völkerrechts. Bd., 1. H., 46*, 42–73.

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review, 22*(3), 1–25. Recuperado em 22 de novembro de 2020, de https://academic.oup.com/isr/article-abstract/22/3/482/5488469?redirectedFrom=fulltext.

Land, M. K. (2016). A human rights perspective on US constitutional protection of the internet. In: *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe. Londres e Nova Iorque*. 48–70. Routledge Taylor and Francis Group.

Lee A. B. (2014) 'Data Privacy Law: An International Perspective', Oxford University Press, 63.

Lessig, L. (1996). Reading The Constitution in Cyberspace. *Emory Law Review, 45*, 869–910.

Lima, C.C.C. (2014). *Marco Civil da Internet: Garantia da privacidade e dados pessoais à luz do marco civil da internet.* Leite, GS., & Lemos, R (coord.). São Paulo: Atlas, 2014.

Mattiuzzo, M. (2018). *Privacidade em perspectivas: Business Models and Big Data: How Google uses your Personal Information*. Branco, S., & Teffé, C. (orgs). Rio de Janeiro: Lumen Juris.

Mendes, L.S., & Mattiuzzo, M. (2019). Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. *Revista Direito Público, 16*(90), 39–64.

Mendonça, R. (2018). *Como os testes de Facebook usam seus dados pessoais - e como empresas ganham dinheiro com isso*. Recuperado em 10 de novembro de 2020, de http://www.bbc.com/portuguese/salasocial-43106323.

Milakovich, M. (2012). Digital Governance: New Technologies for Improving Public Service and Participation. London and New York: Rutledge.

Milakovich, M., &. Gordon, GJ. (2013). *Public Administration in America* (11th ed.) Boston: Cengage Learning.

Möller, K. (2012). *The Global Model of Constitutional Rights.* Oxford: Oxford University Press.

Moncau, L. F. M., & Arguelhes, DW. (2020). The Marco Civil da Internet and Digital Constitutionalism. *In:* Frosio, G. (ed.). *The Oxford Handbook of Online Intermediary Liability* (no prelo). Oxford: Oxford University Press.

Monducci, J. (2003). *Diritti della persona e trattamento dei dati particolari.* Milão: Giuffrè.

Monteiro, R. L. (2019). *A nova Regulação de Proteção de Dados Pessoais aprovada na União Europeia e sua influência no Brasil.* Recuperado em 19 de dezembro de 2020, de https://renatoleitemonteiro.jusbrasil.com.br/artigos/273633610/a-nova-regulacao-deprotecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil.

Morais, J. L. B, & Menezes Neto, EJ. de. (2014). *Marco Civil da Internet: A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance*: Leite, GS., & Lemos, R. (coord.). São Paulo: Atlas.

Morelli, A., & Pollicino, O. (2020). Metaphors, Judicial Frames and Fundamental Rights in Cyberspace. *American Journal of Comparative Law, 2*, 1–26.

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, Massachusetts: The MIT Press.

Padovani, C., & Santaniello, M. (2018). Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system. *International Communication Gazette, 80*(4), 295–301.

Parlamento Europeu. *Diretiva nº 46, de 24 de outubro de 1995. Jornal Oficial das Comunidades Europeias. [S. l.], 23 nov. 1995.*

Parlamento Europeu. *Regulamento nº 679, de 27 de abril de 2016. Jornal Oficial da União Europeia. [S. l.], 04 maio 2016. p. 1-88.*

Pereira, A. P. (2019). *O que é algoritmo?* Recuperado em 27 de maio de 2020, de https://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm.

Pettrachin, A. (2018). Towards a universal declaration on internet rights and freedoms? *International Communication Gazette, 80*(4), 337–353.

Philipp, J. (2016). *Article: "The EU´s New Data Protection Law – How A Directive Evolved Into A Regulation*", Oxford.

Pinheiro, A. S. (2015). *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional.* Lisboa: AAFDL.

Pinheiro, P. P. G. (2019). Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. *Revista dos Tribunais, 1000*, 309-323.

Pollicino, O., & Romeo, G. (2016). *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe. Londres e Nova Iorque.* Routledge Taylor and Francis Group.

Proxxima. (2018). *Uso de algoritmos acontece na economia, política, entretenimento ... e marketing: Dados moldam produtos de empresas como Facebook, Google, Netflix e Amazon, mas também são utilizados em várias outras áreas da atividade humana. Veja Infográfico.* Recuperado em 09 de dezembro de 2019, de http://www.proxxima.com.br/home/proxxima/howto/2018/03/27/uso-de-algoritmos-acontece-na-economia-politica-entretenimento-emarketing.html.

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5, 2021; Published by the Minister of Justice Canadá; Recuperado em 08 de janeiro de 2020, de http://laws-lois.justice.gc.ca.

Quelle, C. (2017) *The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It*, Too. In: Leenes R, van Brakel R, Gutwirth S, De Hert P (eds) Data Protection and Privacy: The Age of Intelligent Machines, pp. 33–62. Hart Publishing, Oxford.

Reidenberg, J. R. (2000). Resolving conflicting international data privacy rules in cyberspace. *Stanford Law Review*, *52*.

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 de Proteção de Dados).* Jornal Oficial L. 2016; 119. Recuperado em 17 de janeiro de 2019, de https://op.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1.

Resolução Legislativa do Parlamento Europeu, de 12 de março de 2014. *Sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados).*

Rodotà, S. (2008). *A vida na sociedade da vigilância: a privacidade hoje.* Rio de Janeiro: Renovar.

Rouvroy A., Poullet Y. (2009) The Right to Informational Self-Determination and the Value of Self-Development: *Reassessing the Importance of Privacy for Democracy. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?.* Springer, Dordrecht. Recuperado em 05 de maio de 2020, de https://doi.org/10.1007/978-1-4020-9498-9_2.

Sajó, A., & Ryan, C. (2016). Judicial reasoning and new technologies: Framing, newness, fundamental rights and the internet. In: *The Internet and Constitutional Law: The protection of fundamental rights and constitutional adjudication in Europe*. 3–25. Londres e Nova Iorque. Routledge Taylor and Francis Group.

Santaniello, M., Palladino, N., Catone, MC., & Diana, P. (2018). The language of digital constitutionalism and the role of national parliaments. *International Communication Gazette*, *80(*4), 320–336.

Santos, A. (2018). Privacidade em perspectivas: *O Impacto do Big Data e dos Algoritmos nas Campanhas Eleitorais.* Organizadores: Sérgio Branco S, & Teffé, C. Rio de Janeiro: Lumen Juris.

Sarlet, I. W., & Hartmann, IAM. (2019) A. Direitos fundamentais e direito privado: a proteção da liberdade de expressão nas mídias sociais. *Revista Direito Público, 16*(90), 85–108.

Sartor, G. (2017). Human Rights and Information Technologies. In: *The Oxford Handbook of Law, Regulation and Technology*. Edited by Roger Brownsword, Eloise Scotford, and Karen Yeung. 425–448. Oxford: Oxford University Press. Recuperado em 02 de julho de 2019, de https://www.oxfordhandbooks.com.

Schulz, W. (2018). Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG. HIIG *Discussion Paper Series*, *1*(1), 15. Recuperado em 18 de novembro de 2019, de https://papers.ssrn.com/abstract=3216572.

Schwartz, P., & Solove, D. (2011). 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information'. *New York University Law Review, 86,* 1814.

Simoncini, A. (2016). *The constitutional dimension of the internet: some research paths*. EUI Department of Law Research Paper, 16. Recuperado em 04 de setembro de 2019, de https://ssrn.com/abstract=2781496.

Solove, D. & Hartzog, W. (2014). *The FTC and the New Common Law of Privacy*, 114, Colum. L. Rev. 583, 587.

Soprana, P. (2018). *O que é a GDPR, a lei de proteção de dados europeia, e por que ela importa*. Recuperado em 21 de março de 2020, de https://gizmodo.uol.com.br/lei-proteca-dados-gdpr/.

Souza, C. A. P. de. *Responsabilidade civil dos provedores de acesso e de aplicações de internet: evolução jurisprudencial e os impactos da Lei 12.695/2014 (Marco Civil da Internet).* In: Leite, GS., & Lemos, R. (coordenadores). 791–817. São Paulo: Atlas.

Sullivan, K. M. (2003). 'Under a watchful eye: *incursions on personal privacy*' in: Leon, R.C., & Anrig, G (orgs.). The War on our freedoms: civil liberties in an age of terrorism (The Century Foundation, Nova York. 128, 131.

Sunstein, C. R. (1996). *Constitutional Caution The Law of Cyberspace.* 361–375. University of Chicago Legal Fórum.

Szeto, M., & Miri, A. (2007). *Analysis of the use of privacy-enhancing technologies to achieve PIPEDA compliance in a B2C e-business model*. In Management of eBusiness, Eighth World Congress.

Tene, O., & Polonetsky, J. (2013). 'Big Data for All: Privacy and User Control in the Age of Analytics'. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), 239.

Teubner, G. (2016). *Fragmentos constitucionais: constitucionalismo social na globalização.* São Paulo: IDP/Saraiva.

Teubner, G. (2017). Horizontal effects of constitutional rights in the internet: a legal case on the digital constitution. *Italian Law Journal*, *3*(2), 485–510. Tratado sobre o funcionamento da União Europeia, 2009, versão consolidada. Jornal Oficial Recuperado em 02 de outubro de 2019, de https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:326:FULL:PT:PDF.

Thomas, G. A., & Jajodia, S. (2004). "Commercial Offthe-Shelf Enterprise Resource Planning Software Implementations in the Public Sectors: Practical Approaches for Improving Project Success." Journal of Government Financial Management, 53.

United Kingdom. *Data Protection Act, de julho de 1998. The Stationery Office. 9th Impression. Londres, abr. 2005.*

Viellechner, L. (2019). The transnational dimension of constitutional rights: Framing and taming "private" governance beyond the state. *Global Constitutionalism, Cambridge University Press, 8*(3), 639–661.

Waldman, A. E. (2018). *Privacy's Law of Design.* Rochester, NY: Social Science Research Network. Recuperado em 18 de fevereiro de 2020, de https://papers.ssrn.com/abstract=3263000.

Yilma, K. M. (2017). Digital privacy and virtues of multilateral digital constitutionalism-Preliminary thoughts. *International Journal of Law and Information Technology*, *25*(2), 115–138.