UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE DIREITO
CURSO DE GRADUAÇÃO EM DIREITO

FERNANDA GOMES ALMEIDA

A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL AUTONÔMO NA ATUAL SOCIEDADE DA INFORMAÇÃO

Salvador/BA
2019

FERNANDA GOMES ALMEIDA

A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL AUTONÔMO NA ATUAL SOCIEDADE DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Federal da Bahia, como requisito parcial para a obtenção do grau de Bacharela em Direito.

Orientadora: Professora Dra. Maria Elisa Villas-Bôas.

Salvador/BA
2019

FERNANDA GOMES ALMEIDA

A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL AUTONÔMO NA ATUALSOCIEDADE DA INFORMAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Federal da Bahia, como requisito parcial para a obtenção do grau de Bacharela em Direito.

Orientadora: Professora Dra. Maria Elisa Villas-Bôas.

Aprovada em _____ de _____ de 2019.

_____

Profª Dra. Maria Elisa Villas-Bôas– Orientadora
Universidade Federal da Bahia

_____

Profº Dr. André Luiz Batista Neves
Universidade Federal da Bahia

_____

Profº Dr. Carlos Eduardo Behrmann Rátis Martins
Universidade Federal Bahia

DEDICATÓRIA

Aos meus pais, familiares, amigos e professores. E a todos as pessoas que, de alguma forma, me ajudaram chegar até aqui. A conquista é nossa!

AGRADECIMENTOS

Agradeço a Deus, pela dádiva da vida. Por me ajudar a encontrar força e coragem nos momentos de medo e insegurança.

Aos meus pais, por tudo. Os sacrifícios enfrentados ao longo da vida para educar e criar os filhos não foram poucos, mas valeram a pena. O meu amor por vocês é imensurável. Obrigada pelo carinho, amor, afeto e cuidado.

Aos meus irmãos pelo apoio constante e palavras de carinho.

À minha querida avó que, por diversas vezes, internalizou as minhas preocupações como se suas fossem.

A Felipe, por acreditar em mim sempre, quando nem eu mesmo acreditei.

Aos amigos queridos que, igualmente atribulados com essa fase final do curso, me enviaram mensagens e energias positivas constantemente, assim como me ajudaram em diversos momentos.

À Professora Maria Elisa Villas-Bôas, que, além da orientação excepcional ao longo do semestre, me deu verdadeiros ensinamentos para a vida. Agradeço pela paciência constante. Sempre após os nossos encontros, me sentia mais calma e confiante. Obrigada por tanto!

"A verdade é que não visamos igualmente todos os eleitores. A maior parte dos nossos recursos foi para visar àqueles que podiam mudar de ideia, os persuasíveis. Nós os bombardeamos com blogs, anúncios, artigos nos sites, vídeos, todas as formas que possa imaginar. Até que vissem o mundo como nós queríamos. Até que votassem no nosso candidato. Como um bumerangue, você envia os seus dados, eles são analisados e volta para você como uma mensagem direcionada para mudar seu comportamento."

(Brittany Kaiser. Ex-diretora da empresa Cambridge Analytica)

RESUMO

O surgimento das novas das tecnologias da informação, no final do século XX, afetou sobremaneira a organização social contemporânea e permitiu a vigilância constante dos indivíduos, que recebem, constantemente, novas ameaças aos seus direitos fundamentais. A noção de privacidade já não é mais suficiente para proteger plenamente os indivíduos na sociedade da informação, devido à ampliação dos riscos de lesão aos direitos individuais, fazendo surgir uma nova instância protetiva, qual seja, o direito à proteção de dados pessoais. Esta monografia busca analisar como se configura o novo direito, que ora se entende por fundamental, especialmente quando considerada a nova era informacional. Assim, busca-se desenvolver um estudo em perspectiva interdisciplinar, por meio de pesquisa bibliográfica, através de raciocínio dedutivo e método jurídico exploratório. Desse modo, primeiramente, será desenvolvido um estudo acerca da atual sociedade da informação, analisando-se, a partir de uma perspectiva histórica, como os indivíduos passaram a ser constantemente monitorados. Serão examinados alguns dos impactos das novas tecnologias na sociedade contemporânea e, por conseguinte, serão analisadas as principais previsões normativas, internacionais e nacionais, acerca do tema, destacando-se, de forma mais pormenorizada, o Regulamento Europeu, o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. Serão investigados, ainda, os principais direitos fundamentais envolvidos, assim como os riscos a que estão submetidos os indivíduos quando do processamento indevido dos seus dados. Por fim, serão destacadas as principais características do novel direito, realizando-se um estudo acerca do recente Projeto de Emenda Constitucional nº 17/2019 que, caso entre em vigor, alterará o texto constitucional para abarcar, no rol de direitos fundamentais, a proteção de dados pessoais como um direito autônomo.

Palavras-Chave: proteção de dados; direitos fundamentais; sociedade da informação.

ABSTRACT

The emergence of new information technologies at the end of the twentieth century greatly affected contemporary social organization and allowed the constant vigilance of individuals, who constantly receive new threats to their fundamental rights. The notion of privacy is no longer sufficient to fully protect individuals in the information society, due to the increased risk of damage to individual rights, giving rise to a new protective instance, namely the right to the protection of personal data. This monograph seeks to analyze how the new right is configured, which is now understood as fundamental, especially when considering the new information age. Thus, we seek to develop a study in an interdisciplinary perspective through bibliographic research, through deductive reasoning and exploratory legal method. Thus, firstly, a study about the current information society will be developed, analyzing, from a historical perspective, how individuals have been constantly monitored. Some of the impacts of new technologies on contemporary society will be examined and the main international and national normative forecasts on the subject will be analyzed. The European Regulation, the Internet Framework and the the General Personal Data Protection Act. It will also investigate the main fundamental rights involved, as well as the risks to which individuals are subjected when improperly processing their data. Finally, the main features of the novel law will be highlighted, by conducting a study on the recent Draft Constitutional Amendment No. 17/2019 which, if it enters into force, will amend the constitutional text to encompass the protection of fundamental rights of personal data as an autonomous right.

Keywords: data protection; fundamental rights; information society.

LISTA DE ABREVIATURAS E SIGLAS

§	PARÁGRAFO
ART.	ARTIGO
CDC	CÓDIGO DE DEFESA DO CONSUMIDOR
DPA	DATA PROTECTION AUTHORITIES
GDPR	GENERAL DATA PROTECTION REGULATION
LCP	LEI DO CADASTRO POSITIVO
LGPD	LEI GERAL DE PROTEÇÃO DE DADOS
MCI	MARCO CIVIL DA INTERNET
Nº	NÚMERO
OCDE	ORGANIZAÇÃO PARA COPERAÇÃO E DESENVOLVIMENTO ECONÔMICO
RGPD	REGULAMENTO GERAL DE PROTEÇÃO DE DADOS
UE	UNIÃO EUROPEIA

SUMÁRIO

1 INTRODUÇÃO

Diante da recente evolução tecnológica, os dados pessoais passaram a ser transmitidos, processados e armazenados de forma revolucionária, nunca antes vista na história da humanidade. Governos e iniciativa privada, com intuito de melhor conhecer os cidadãos, aprimorar serviços, otimizar resultados e gerar lucros, passaram a monitorar diuturnamente os indivíduos, por meio das chamadas tecnologias da informação. Apesar dos avanços históricos possibilitados com o advento de tal estrutura social, econômica e política, verifica-se que os cidadãos estão, cada vez mais, expostos a inúmeros riscos provenientes do processamento massivo de suas informações pessoais.

Dessa forma, os indivíduos não logram mais êxito em defender e controlar os seus próprios dados, fato esse que pode acarretar violação a diversos direitos fundamentais, que representam valores caros à existência humana. Assim, privacidade, imagem, honra, dignidade da pessoa humana, igualdade, devido processo legal, autonomia e liberdade de pensamento, dentre outros tantos direitos previstos na Carta Magna, podem ser facilmente atingidos, principalmente após o advento e massificação da *internet.* É necessário, portanto, o advento de mecanismos que possibilitem aos cidadãos deter conhecimento acerca da utilização dos seus dados pelos mais variados setores da sociedade, possibilitando-se a eles um verdadeiro poder de autodeterminação informacional.

À vista disso, tem-se que o direito fundamental à privacidade, habitualmente relacionado à proteção de dados pessoais, não é suficiente para salvaguardar os indivíduos, de forma plena, na atual sociedade da informação. O seu âmbito de proteção, limitado às informações íntimas e privadas, está longe de abarcar todos os riscos proporcionados pelo processamento automatizado de dados. Diante de tal insuficiência normativa, surge o seguinte questionamento: a proteção de dados pode ser vista como um direito fundamental autônomo?

Para tanto, utilizou-se da técnica de pesquisa bibliográfica, uma vez que foram analisados livros, artigos científicos, revistas, documentos eletrônicos e artigos provenientes do meio virtual. Fez-se uso de doutrina e jurisprudência, nacional e estrangeira, assim como se desenvolveu um estudo interdisciplinar, abarcando conteúdos de direito constitucional, direito digital e ciência sociológica. O tipo de

raciocínio desenvolvido foi o dedutivo, em que se partiu de análises generalizadas acerca da noção da proteção de dados pessoais, para, então, individualizar o problema da proteção de dados como um direito fundamental autônomo. Ainda, detectou-se que a investigação foi feita pelo método jurídico exploratório, visando a proporcionar maior familiaridade com o problema ora estudado, tornando-o compreensível e construindo-se hipóteses sobre ele por meio de levantamento bibliográfico.

Desse modo, o trabalho está estruturado em três capítulos. No primeiro, traçar-se-á um panorama geral acerca da sociedade da informação, sendo abordada a evolução histórica pela qual passou a humanidade até chegar ao atual nível tecnológico. Analisar-se-ão as principais características de tal sociedade, bem como os aspectos que permitem uma vigilância constante sobre os indivíduos, apta a violar diversos direitos fundamentais. No segundo capítulo, far-se-á um breve estudo acerca do conceito e espécies de dados pessoais, dos principais princípios atinentes ao tema e das principais normas, nacionais e internacionais, que regulam o tratamento de dados. Destinar-se-á o terceiro ao estudo da proteção de dados como um direito fundamental autônomo, desvinculado do direito fundamental à privacidade, assim como da Proposta de Emenda Constitucional 17/2019.

Por fim, apresentar-se-ão as conclusões decorrentes da presente pesquisa.

2 SOCIEDADE DA INFORMAÇÃO

A compreensão da revolução tecnológica e do surgimento da sociedade da informação é de vital importância para o melhor entendimento do tema ora abordado nessa pesquisa. Faz-se necessário entender as transformações ocorridas na sociedade no decorrer do tempo, analisando os mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação (CASTELLS, 2000). Dessa forma, sabe-se que, nas últimas décadas, as informações passaram a ser transmitidas, armazenadas e utilizadas de forma cada vez mais ampla, transfronteiriça, gerando um fluxo informacional que já não encontra mais obstáculos físicos distanciais (BIONI, 2019).

Assim, para melhor caracterização do atual estágio de desenvolvimento, é indispensável o exame dos diferentes modos de organização social vividos pela sociedade ao longo da história da humanidade, sendo pacífica, entre os doutrinadores, a divisão de tais modos em três grandes momentos: sociedade agrícola, sociedade industrial e a atual sociedade da informação (SILVA, 2009).

2.1 DA SOCIEDADE AGRÍCOLA À SOCIEDADE DA INFORMAÇÃO

A sociedade agrícola se caracterizou pela fixação do homem em locais determinados, sendo o cultivo da agricultura a grande fonte de riqueza. Os produtos agrícolas tinham significativo valor e os meios de troca ganharam força através do escambo, surgindo, assim, as primeiras práticas comerciais. Com o aprimoramento das técnicas de produção, chega-se ao momento da utilização das máquinas a vapor e, posteriormente, da descoberta da eletricidade, eventos que fizeram disparar a Revolução Industrial, inaugurando-se uma nova era de produção de riquezas na sociedade mundial (SILVA, 2009).

Já nessa época de intensa industrialização, nos séculos XVIII e XIX, houve o repentino aumento de aplicações tecnológicas, responsável pela transformação dos processos de produção e distribuição dos bens, criação de novos produtos bem como pela mudança da localização das riquezas, que ficou apenas ao alcance dos países e elites capazes de comandar tal sistema tecnológico (CASTELLS).

Nos dizeres de Manuel Castells,

> Portanto, atuando no processo central de todos os processos – ou seja, a energia necessária para produzir, distribuir e comunicar – as duas Revoluções Industriais difundiram-se por todo o sistema econômico e permearam todo o tecido social. Fontes móveis de energia barata e acessível expandiram e aumentaram a força do corpo humano, criando a base material para a continuação histórica de um movimento semelhante rumo à expansão da mente humana. (2000, p. 75).

Cresce, assim, a utilização de novas tecnologias, a comunicação e integração entre os povos, a difusão da mídia e a valorização do capital humano ou intelectual, fazendo surgir um novo tipo de sociedade. Assim, essa pode ser compreendida como uma nova forma de organização social, econômica e política que recorre ao intenso uso de tecnologia para coleta, produção, processamento, transmissão e armazenamento de informações (VIEIRA T., 2007).

Como bem observa Manuel Castells (2000), dentre as tecnologias da informação incluem-se o conjunto convergente de técnicas em microeletrônica, computação (software e hardware), telecomunicações/radiofusão, optoeletrônica, bem como a engenharia genética e seu vasto campo de aplicação. Tais ciências, que se difundiram ao redor do mundo precipuamente no final do século XX, são, para essa revolução tecnológica, o que as fontes de energia foram para as revoluções industriais e o que a terra e a agricultura foram para a sociedade agrícola.

De acordo com Paulo Hamilton Siqueira Jr.,

> A sociedade da informação é constituída em tecnologias de informação e comunicação que envolve a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos, como rádio, televisão, telefone e computadores, entre outros. Essas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, econômicos e políticos, criando uma nova estrutura social, que tem reflexos na sociedade local e global (...). A “sociedade da informação” tem como principal valor a informação, o conhecimento. Na era agrícola, a terra se configurava como o fator primordial para a geração de riquezas. Na era industrial a riqueza surge da máquina a vapor e da eletricidade. Na era do conhecimento, a informação e o conhecimento são os atores centrais da produção econômica. (2012, p. 236-240).

Já se falava da importância da informação no seio das sociedades: tanto a revolução agrícola quanto a revolução industrial causaram impactos na sua agilidade e transmissibilidade. Assim, na sociedade industrial, era perceptível o valor da informação para aperfeiçoar o desenvolvimento econômico, acelerar a produção, alcançar melhores taxas de produtividade, bem como aumentar, de forma

considerável, a geração de riquezas. *Per si*, ela não é a grande novidade da era atual. O papel de destaque, portanto, refere-se aos mecanismos que permitiram o seu processamento e transmissão em quantidade e velocidade jamais imaginável (BIONI, 2019).

Pode-se dizer que vivemos a era da mais importante revolução tecnológica, nunca antes experimentada. As distâncias de tempo e espaço foram drasticamente encurtadas, produzindo diversas consequências sobre as concepções de território, política, soberania, economia e cultura, atingindo áreas geográficas mais extensas bem como maior número de pessoas (PAESANI, 2007). Cita-se, como exemplo, as manifestações de junho de 2013, que se iniciaram em São Paulo e no Rio de Janeiro, contra o aumento das tarifas de ônibus. O exercício da cidadania foi revitalizado por um amplo fluxo informacional, que teve como principal consequência à conexão entre milhares de manifestantes localizados em todo o território nacional, facilitando sobremaneira a organização e disseminação dos protestos. Em poucos dias, as reivindicações cresceram de tal forma que extrapolaram os 20 centavos do aumento da tarifa, e tornaram-se verdadeiras exigências por melhorias sociais. A rede tornou-se, assim, um verdadeiro instrumento de engajamento social (BIONI, 2019. p. 5), modificando as formas de exercício de cidadania ao redor de todo o mundo.

Cumpre ressaltar que, por detrás de tal revolução, existem imensas malhas de meios de comunicação interligando países e continentes, fios de telefone, canais de microondas, linhas de fibra ótica, cabos submarinos transoceânicos, transmissões via satélite, e diversos outros aparatos tecnológicos que formam uma “superestrada”, também denominada de “infovia” ou “supervia”, permitindo uma maciça troca de informações e serviços (TAKAHASHI, 2000). Portanto, a revolução tecnológica produziu o encolhimento do mundo justamente pelo encurtamento do tempo (PAESANI, 2007), facilitando a integração em rede e transformando a informação em recurso indispensável para o fluxo da economia e para geração de riqueza, como se verá mais adiante.

2.2 CARACTERIZANDO A SOCIEDADE DA INFORMAÇÃO

Na sociedade atual, o desenvolvimento e o progresso social encontram-se calcados em bens imateriais, dados, bem como conhecimentos científicos e tecnológicos. Nessa esteira, Manuel Castells (2000) destaca os aspectos centrais do paradigma da tecnologia da informação, que representam a base material da nova estrutura social. Segundo o autor, a *primeira característica* do novo paradigma se encontra no fato de a informação ser matéria-prima, a mola propulsora para a geração de riqueza. A *segunda característica* reside no fato da "*penetrabilidade dos efeitos das novas tecnologias"*, uma vez que toda a coletividade é moldada por estes novos meios tecnológicos, sendo a informação parte integral de toda a atividade humana. A *terceira característica* seria a *lógica de redes*, vez que a rede pode ser implementada em todos os tipos de organizações e processos. A *quarta característica* consiste na *flexibilidade*, destacando-se a capacidade de reconfiguração do novo paradigma tecnológico, aspecto este decisivo para uma sociedade caracterizada por fluidez e constantes mudanças. Por fim, a *quinta característica* é a *crescente convergência de tecnologias específicas para um sistema altamente integrado,* em que não é mais possível diferenciar, em separado, as diferentes tecnologias da informação, existindo uma verdadeira integração entre microeletrônica, telecomunicações, optoeletrônica e computadores.

Enganam-se, entretanto, os que pensam que tal revolução é democrática e inclusiva. Há grandes áreas do mundo e consideráveis segmentos da população que estão desconectados do atual sistema tecnológico (CASTELLS, 2000), existindo uma verdadeira cisão global entre países "ricos em informação" e "pobres em informação", conforme relatório da Organização das Nações Unidas – ONU, de julho de 1999, intitulado *Globalization with human* (VIEIRA T., 2007, p. 161). Dessa forma, de um lado, há os países que produzem conhecimento, através da coleta e processamento dos mais variados tipos de informação, realizam pesquisa, criam produtos e serviços e os distribuem, fazendo parte do setor dominante do mundo globalizado. De outro, encontram-se os países que, por não serem tecnologicamente desenvolvidos, apenas "consomem" as pesquisas, produtos e serviços produzidos pelos primeiros (VIEIRA T., 2007, p. 161). Assim, muitas regiões e populações estão, atualmente, excluídas de tal ambiente informacional (SIQUEIRA, 2012), intensificando o panorama de desigualdade social, econômica, política e tecnológica.

Como bem observa Pierre Lévy (1999), o acesso ao ciberespaço exige uma infraestrutura tecnológica de custo alto para as regiões em desenvolvimento, devendo existir investimentos consideráveis para montagem e manutenção dos servidores. Somado a isso, há um crescente sentimento de incompetência e desqualificação de tais países frente às novas tecnologias. De acordo com Patrícia Peck Pinheiro,

> Na Agenda 2030 para o Desenvolvimento Sustentável da Organização das Nações Unidas (ONU), os Estados-membros reconheceram a importância da expansão das tecnologias da informação, das comunicações e da interconexão mundial, destacando a necessidade de enfrentar as profundas desigualdades digitais e desenvolver as sociedades do conhecimento, com base em uma educação inclusiva, equitativa, não discriminatória, com respeito às diversidades culturais. (2018, p. 213).

Ademais, surge uma nova especialidade, denominada “segurança da informação”, responsável por assegurar a disponibilidade, integridade, autenticidade e confidencialidade das informações. Segundo Tatiana Vieira, a importância de tal campo pode ser assim resumida:

> Por *disponibilidade* entende-se a possibilidade de acesso e utilização oportunos de informações por indivíduos e sistemas autorizados. *Integridade* significa que a informação não foi modificada, inclusive quanto à origem e ao destino. *Autenticidade* quer dizer que a informação foi produzida, expedida, recebida, modificada ou destruída por determinado indivíduo ou sistema. Por fim, *confidencialidade* significa acesso ou divulgação restrito, ou seja, sigilo. Hoje, a *segurança da informação* está sendo implementada tanto pelo setor privado – como forma de garantir a continuidade do negócio, minimizar os riscos e maximizar os investimentos – como pelo setor público – especialmente para garantir a disponibilidade e a integridade dos documentos públicos, para controlar o acesso às informações sigilosas e para incrementar as atividades de governo eletrônico. (2007, p. 161).

Outra característica refere-se à crescente massa de trabalhadores desempregados, que são eliminados devido às mais variadas inovações tecnológicas. Surge para as empresas a possibilidade de contratação à distância de profissionais capacitados - até mesmo em países em que a mão-de-obra é mais barata -, sendo ofertada a opção do “teletrabalho” (VIEIRA T., 2007, p. 162). Nesse quadro, torna-se extremamente necessário “ampliar a empregabilidade dos trabalhadores, por meio de aprendizado continuado e do desenvolvimento de novas habilidades e competências [...]” (TAKAHASHI, 2000, p. 7), oportunizando-se, diuturnamente, a possibilidade de reciclagem de suas habilidades.

Nesse contexto, destaca-se, ainda, o intenso uso de aparatos tecnológicos pelo setor privado: as empresas utilizam a rede como principal meio de comunicação e processamento de informações, fato que transformou consideravelmente a prática empresarial. É nessa nova era que surgem os negócios eletrônicos (*e-business*), dentre os quais se destaca o comércio eletrônico (*e-commerce*), indispensáveis para a modernização do setor produtivo, bem como o aperfeiçoamento das atividades negociais. Assim, tanto os produtores de bens e serviços quanto os consumidores devem estar capacitados e conectados às redes digitais, para operá-las adequadamente (VIEIRA T., 2007). As tecnologias da informação e comunicação serviram, portanto, para "divulgação de negócios, comunicação mais rápida e barata, acesso a informações úteis, agilidade nas compras e vendas, ampliação de mercados e diminuição de custos operacionais" (TAKAHASHI, 2000, p. 6).

No âmbito público, visando à modernização do Estado, os governos investem em diversas tecnologias, objetivando a diminuição da burocracia, a redução de custos, a transparência dos gastos, o aperfeiçoamento na prestação de serviços públicos, bem como o melhor relacionamento entre cidadãos e administração pública. Assim, algumas atividades envolvem o fornecimento *online* de certidões, a tramitação eletrônica de documentos públicos, a criação de portais com informações úteis para toda a população, a orientação dos cidadãos quanto a serviços públicos relevantes, a educação, o pregão eletrônico, integração entre os mais variados órgãos governamentais, dentre outros (VIEIRA T., 2007). Destaca-se, dessa forma, o uso das tecnologias para possibilitar uma administração pública mais transparente e eficaz, voltada ao aperfeiçoamento da própria gestão do governo - planejamento, coordenação, controle e execução de ações, contabilidade pública, aumento da participação democrática e etc. (TAKAHASHI, 2000).

Isso posto, cumpre dizer que tais tecnologias ocupam o centro da dinâmica de inovações, sendo fatores primordiais para o crescimento econômico, competitividade, geração de riquezas, compartilhamento de conhecimentos, informações e dados. Surgem, no entanto, novas preocupações envolvendo a segurança nas redes, vez que a crescente utilização de recursos computacionais por governos, empresas e cidadãos implica diversas vulnerabilidades, possibilitando a exploração de falhas dos sistemas e ameaças por indivíduos mal intencionados. Como bem observa Tatiana Vieira,

> A capacidade de se obter uma informação crítica, poluir bancos de dados ou devastar sistemas-chave de comunicação torna-se uma arma nesse novo ambiente tecnológico. Quanto mais um governo e uma sociedade dependem de sua rede de comunicação, maior sua exposição a ataques de *hackers,* de *crackers*[1] e de organizações criminosas. Cresce, portanto, a incidência dos denominados *cybercrimes*, ou seja, crimes cometidos em meio eletrônico (...). Tornam-se cada vez mais comuns os ilícitos praticados em meio digital, materializados tanto no acesso indevido a informações armazenadas em bancos de dados ou transmitidas por meio de sistemas informatizados (violação da confidencialidade); quanto na alteração de dados armazenados em bancos de dados ou transmitidos por sistemas de comunicação eletrônica (violação da integridade); sem falar na falsificação de identidade e de dados (violação da autenticidade); estelionatos eletrônicos (*phishing scams*); na pornografia infantil, no racismo e na xenofobia; no atentado à propriedade intelectual e aos direitos conexos; nos danos por difusão de vírus; na invasão de privacidade; e na violação de sigilo industrial. (2007, p. 163-164).

Nesse contexto, as ameaças e danos advindos da má utilização das redes de comunicação revelam-se mais difíceis do que os advindos do mundo real. O rastreamento, a captura e condenação de criminosos, que possuem como principal arma a tecnologia da informação, são extremamente complexos, vez que o atacante dispensa a proximidade física com as suas vítimas, podendo situar-se em qualquer lugar do mundo e atacar computadores onde quer que estejam (VIEIRA T., 2007). De acordo com Patrícia Peck Pinheiro,

> Com isso presenciamos o crescimento de ocorrências e quadrilhas especializadas no ambiente digital. Todavia, mais de 60% das organizações nacionais não possuem programas para prevenir ameaças de acordo com a Global Information Security Survey (GISS). O estudo anual da Ernst & Young aponta que 43% das empresas não têm um programa para identificação de vulnerabilidades e 45% não dispõem de nenhum tipo de programa para detecção de brechas. Aumentaram também os casos de ofensas, racismo e intolerância, chegando ao extremo de os serviços digitais serem usados por movimentos terroristas para propagar ideologias e recrutar seguidores, desafiando governos e ONG's. Afinal, as redes sociais são uma maneira extremamente efetiva de transmitir uma mensagem a um público-alvo. (2018, p. 87).

Ademais, destaca-se o intenso uso de aparatos tecnológicos para supervisionar e fiscalizar ações dos indivíduos, assim como para armazenar dados pessoais a baixos custos e de maneira facilitada. Diferentes empresas coletam, cotidianamente, informações pessoais, que são cruzadas "com dados provenientes

[1] "Hackers" e "Crackers" se referem a indivíduos com habilidades avançadas em computadores, de uma maneira geral. Entretanto, o primeiro grupo dedica o seu tempo a conhecer e modificar softwares, hardwares e rede de computadores, acessando dispositivos sem a devida autorização. O segundo grupo, por sua vez, se utiliza da tecnologia para quebrar sistemas de segurança visando quebrar ou remover dados, utilizando-se do seu conhecimento para gerar danos. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/hackers_crackers_qual_a_diferenca_entre_eles.html#rmcl. Acesso em: 25 nov. 2019.

de prestadoras de serviço telefônico, provedores de acesso à internet, administradoras de cartão de crédito, bancos, enfim, toda e qualquer organização que possa contribuir para o processo de delineamento do perfil das pessoas" (VIEIRA T., 2007, p. 175).

Pode-se dizer que as grandes vilãs são aquelas empresas que prestam serviços pela *internet* (*empresas.com)* e possuem como principal forma de rendimento a publicidade direcionada e o marketing. O papel de tais companhias é o de monitorar seus clientes quanto à sua localização, preferências, *hobbies* e sites visitados; comprar e vender dados de caráter pessoal; traçar o perfil de potenciais consumidores e comercializar tais informações com diversas prestadoras de serviços, pondo em risco a privacidade dos usuários diante da excessiva acumulação de informações pessoais (VIEIRA T., 2007).

A possibilidade de êxito frente aos consumidores aumentou de forma significativa, vez que as empresas possuem a exata noção da repercussão - positiva ou negativa - de determinado produto ou serviço. As informações pessoais tornaram-se, portanto, extremamente estratégicas e produtivas à atividade empresarial, fazendo David Freedman afirmar que:

> *Google, Yahoo* e outras empresas precisam saber quem você é; onde você está; o que você compra; o que você assiste e lê; com quem você divide seu tempo; e até o que você diz aos seus amigos. Mas nenhuma empresa quer ser pega espionando seus clientes, então, essas companhias os importunam e os seduzem literalmente a cada dígito teclado, até que concordem com a coleta de informações necessárias à publicidade personalizada. Devemos aceitar essa situação? Uma vez que a história de sua vida cotidiana está nos bancos de dados do *Google* e de outras empresas, você simplesmente tem que ter confiança que não será disponibilizada para organismos públicos de execução da lei, sua esposa, seu chefe, extorsionistas ou qualquer pessoa que esteja trabalhando contra seus interesses. E por mais que essas companhias sejam confiáveis, elas não terão como evitar o acesso por *hackers* e outras espécies de criminosos.[2] (2006 apud VIEIRA T., 2007, p. 176).

[2] "*Google, Yahoo and others need to know who you are; where you are; what you buy, watch and read; who you spend time with, and even what you say to your friends. No business wants to be caught spying on its customers, of course; these companies plan to nudge and secude us, literally bit by bit, into agreeing to let them gather the information advertisers needed for tailored pitches. (...) Should we put up with it? Once the story of your day-to-day life is on file at Google and other companies, you will simply have to take it on faith that they won't let it get into the hands of law-enforcement agencies, your spouse, your boss, extortionists and anyone else who might be working against your interests. And no matter how trustworthy these companies turn out to be, they might not be able to stop criminal and hackers from lifting the data anyway" (*Tradução livre).

Assim, diversos programas e ferramentas, a exemplo dos *cookies*[3], captam informações dos indivíduos e as gerenciam, objetivando melhor aproveitamento de tudo o que foi obtido com a navegação nas redes. Tais informações são utilizadas e comercializadas para os mais diversos fins, muitas vezes desconhecidos pelo próprio usuário, destacando-se, a publicidade direcionada, bem mais efetiva quando comparada com a abordagem publicitária comum. Frise-se que os próprios cliques permitem mensurar a eficácia de tal publicidade, já que é possível rastrear se os indivíduos realmente se interessaram por aquilo que lhe foi direcionado de acordo com o seu perfil (BIONI, 2019).

Sabe-se, por exemplo, o que a pessoa está lendo, quais os *websites* que acessa, pelo que ela se interessa e o que está mais suscetível a consumir. Tal cenário fez Susanne Lace cunhar a expressão "consumidor de vidro" (LACE, 2005, p.1) que, agora, alcança seu êxito devido ao monitoramento contínuo dos seus hábitos diários, até mesmo de suas emoções. O consumidor tornou-se totalmente transparente (BIONI, 2019).

Assim, após a revolução agrícola e industrial, "*a revolução da tecnologia da informação* se eleva como terceira grande transformação da humanidade" (VIEIRA T., 2007, p. 166-167). O destino das informações pessoais coletadas/capturadas nas redes causa grande preocupação para os cidadãos e até mesmo governos, existindo uma série de regulamentações e leis para determinar direitos e obrigações, bem como o uso ético de dados no âmbito virtual (PINHEIRO, 2018).

Traçado esse panorama geral, entende-se que a principal característica da atual sociedade está na *vigilância imperativa* (BIONI, 2019) dos indivíduos, que já não mais possuem os seus direitos fundamentais resguardados como antes. O cidadão tornou-se mero expectador de suas informações, ocupando uma posição de total passividade nesse novo cenário global. São inúmeros os desafios para proteger tais bens imateriais, intangíveis, tendo em vista o natural "fluxo desses ativos de conhecimento, que se tornaram independentes do suporte físico, principalmente através das fronteiras digitais." (PINHEIRO, 2018, p. 208).

[3] "Trata-se de programas de dados gerados com o objetivo principal de identificação do usuário, rastreamento e obtenção de dados úteis a seu respeito, especialmente, baseada em dados de navegação e de consumo." (MARTINS, 2008, p. 227-228).

2.3 VIGILÂNCIA IMPERATIVA E PRIVACIDADE

Pode-se dizer que, atualmente, a eficiência e o controle estão entre as justificativas para a utilização de informações pessoais tanto pelo Estado quanto por organismos privados. Assim, o setor público se utilizou de censos e pesquisas para melhor conhecer a sua população, objetivando uma administração pública e eficiente. Entretanto, tais informações foram utilizadas, em diversos momentos da história, como forma de controle social sobre os indivíduos, característica essa comum aos governos totalitários.

No âmbito privado, a utilização da informação pessoal inicialmente era limitada e pouco atraente, decorrente da falta de meios e altos custos para a sua coleta. Com o desenvolvimento das tecnologias, em particular o avanço da informática, passaram a ser coletadas por empresas a um custo razoável e utilizadas para uma extensa gama de possibilidades, surgindo uma nova estrutura de poder possibilitada por esta recente arquitetura informacional (DONEDA, 2006).

Tais situações podem ser facilmente ilustradas por meio de dois fatos históricos emblemáticos, que, já naquela época, deixaram evidente a falta de controle dos cidadãos sobre as suas informações pessoais. O primeiro refere-se à Lei do Censo Alemã, de 1983, tendo essa determinado que os cidadãos fornecessem uma série de dados pessoais para fins estatísticos de distribuição geográfica da população (MARTINS, 2005). Tal norma previa, contudo, a possibilidade de cruzamento e comparação dos dados coletados com outros registros públicos, sob o argumento de que tal conduta se fazia necessária para a execução de determinadas atividades administrativas. A finalidade genérica da lei, assim como sua vagueza e amplitude, resultou em uma série de reclamações perante o Tribunal Constitucional Alemão, que declarou a sua inconstitucionalidade parcial e determinou que o compartilhamento dos dados pessoais coletados se destinaria apenas à finalidade de recenseamento (MARTINS, 2005).

Assim, declarou nulos os dispositivos que determinavam a comparação dos dados coletados e a sua transferência a outros órgãos da administração, bem como argumentou acerca da existência de um direito à "autodeterminação informativa" (*informationelle Selbstbestimmung*). Tal julgado, portanto, reverte-se de suma importância, vez que serviu de base para as subsequentes normas nacionais e

europeias e elevou o indivíduo como principal personagem no processo de utilização de seus dados (MENDES, 2014). Com isso, pode-se dizer que:

> (...) o grande mérito do julgamento reside na consolidação da ideia de que a proteção de dados pessoais baseia-se em um direito subjetivo fundamental, que deve ser concretizado pelo legislador e que não pode ter o seu núcleo fundamental violado (...). A Corte afirmou que o moderno processamento de dados pessoais configura uma grave ameaça à personalidade do indivíduo, na medida em que possibilita o armazenamento ilimitado de dados, bem como permite a sua combinação de modo a formar um retrato completo da pessoa, sem a sua participação ou conhecimento (MENDES, 2014, p. 26-27).

Bruno Bioni (2019) destaca a importância do julgado no que se refere ao papel de protagonismo dos cidadãos, que devem ter o controle de seus dados pessoais como forma de autodeterminar as informações que lhes dizem respeito. O autor, a partir de uma releitura do julgado, afirma que a Corte Alemã estabeleceu a base dogmática para a construção da proteção de dados pessoais como um direito da personalidade autônomo, apartado da privacidade, não podendo ser entendido nem mesmo como uma evolução dessa.

O segundo fato emblemático é bem relatado por Arthur Miller (1972 apud DONEDA, 2006), trazendo o autor que, na década de 1960, o departamento do Censo dos Estados Unidos passou a colher dados dos cidadãos norte-americanos acerca de suas habitações, a história pessoal dos próprios ocupantes, chegando a exigir, na década seguinte, os motivos do rompimento de eventuais matrimônios. A melhor maneira de compreender esse processo, segundo Danilo Doneda, é considerar que não houve um crescimento da necessidade do Estado de saber acerca de insucessos matrimoniais de seus cidadãos, mas sim o aperfeiçoamento da tecnologia da época, que tornou factível processar tais informações e delas se extrair alguma utilidade.

Nesse contexto, os pressupostos de eficiência e controle são bem descritos pelo pensador e filósofo francês Michel Foucault (1999), especialmente na sua obra *Vigiar e Punir*, publicada em 1975. O autor escreve acerca do poder disciplinar, que tem por objetivo tornar o indivíduo mais obediente, mediante uma política de total coerção, manipulação e vigilância. Tal poder, exercido pela Igreja por meio de arquivos detalhados acerca da orientação religiosa, hábitos, crenças, práticas e

costumes de comunidades que ameaçavam o seu poderio, passou a ser exercido também pelo Estado.

A vigilância sobre o indivíduo tornou-se constante, seja nas fábricas e escolas, com o monitoramento do tempo de trabalho e estudo, seja em hospitais, hospícios e prisões (VIEIRA T., 2007), bem como ganhou status de operador econômico, devido a sua importância para o funcionamento do poder disciplinar (FOUCAULT, 1999, p. 147). Assim, os ambientes sociais foram reformulados e o poder disciplinar ampliado, criando-se verdadeiros observatórios humanos que vigiavam as pessoas permanentemente para melhor conhecê-las e controlá-las, visto que, quanto maior o número de informações, maior a possibilidade de controle. Segundo Foucault,

> O aparelho disciplinar perfeito capacitaria um único olhar tudo ver permanentemente. Um ponto central seria ao mesmo tempo fonte de luz que iluminasse todas as coisas, e lugar de convergência para tudo o que deve ser sabido: olho perfeito a que nada escapa e centro em direção ao qual todos os olhares convergem. (1999, p. 146).

O modelo arquitetural panóptico, portanto, foi utilizado como forma de garantir constante e detalhada observação de loucos, doentes, condenados, operários, militares e estudantes, sendo o seu principal efeito a criação de um estado de permanente visibilidade, medida que asseguraria o funcionamento do poder. Assim, mais importante do que ser propriamente vigiado é saber que pode estar sendo vigiado: o indivíduo não precisa saber que está sendo vigiado, mas deve ter a certeza que sempre poderá sê-lo (FOUCAULT, 1999).

É necessário entender tal quadro para compreender que o panoptismo é traço característico das sociedades contemporâneas, vez que permite ao Estado e às organizações privadas o monitoramento constante e individual dos cidadãos, abrangendo todas as pessoas, tanto as que exercem o poder como sobre as quais o poder se exerce (VIEIRA T., 2007). Vê-se, pois, que os indivíduos, além de permanentemente monitorados, são classificados em extensos arquivos contendo informações pessoais, podendo-se afirmar que o avanço da tecnologia da informação intensificou o exercício do poder disciplinar, bem como aprimorou os meios para a vigilância constante e universal.

Patrícia Pinheiro (2018) traz exemplos atuais acerca do monitoramento diuturno realizado por grandes empresas sobre os indivíduos, a exemplo do *Google, WhatsApp e Facebook*. Assim, é pertinente trazer à tona trechos de alguns termos

de uso e Políticas de Privacidade de tais empresas, como forma de exemplificar tudo o quanto exposto até o presente momento, ainda que, na prática, raríssimas pessoas os leiam ou deixem de aquiescer. O termo de uso do *Google* pode ser assim resumido:

> Quando você faz o upload, submete, armazena [...] você concede ao Google (e àqueles com quem trabalhamos) uma licença mundial para usar, hospedar, armazenar, reproduzir, modificar, criar obras derivadas (como aquelas resultantes de traduções, adaptações ou outras alterações que fazemos para que seu conteúdo funcione melhor com nossos Serviços), comunicar, publicar, executar e exibir publicamente e distribuir tal conteúdo. [...] Essa licença perdura mesmo que você deixe de usar nossos Serviços [...]. (PINHEIRO, 2018, p. 208-209)

O aplicativo de mensagens *WhatsApp*, adquirido pela empresa *Facebook* no ano de 2014, possui criptografia de ponta a ponta para que as mensagens trocadas pelos usuários possuam maior proteção. Frise-se que a não interceptação de mensagens, quando solicitada por ordem judicial, foi o motivo do bloqueio dos serviços do aplicativo em 2016 e 2017 no Brasil (PINHEIRO, 2018). Entretanto, o aplicativo recebe ou coleta dados pessoais sempre que opera e presta serviços:

> Você concorda com nossas práticas relacionadas a dados, inclusive com a coleta, o uso, o processamento e o compartilhamento de seus dados conforme descrito nesta Política de Privacidade, além da transferência e do processamento de seus dados nos Estados Unidos e em outros países onde temos ou usamos instalações, prestadores de serviço ou parceiros, independentemente do país onde nossos serviços são usados por você. Você reconhece que as leis, regulamentos e normas do país no qual os dados são armazenados podem ser diferentes do que vige em seu próprio país.
> (...)
> Usamos todos os dados em nosso poder para nos ajudar a operar, executar, aprimorar, entender, personalizar, dar suporte e anunciar nossos Serviços. (...) Utilizamos cookies para operar, executar, aprimorar, entender e personalizar nossos Serviços. (...) Mensagens que você possa vir a receber contendo marketing, poderão incluir uma oferta para algo que talvez lhe interesse. (PINHEIRO, 2018, p. 209-210).

A autora destaca o fato de que, quando da instalação do aplicativo, o usuário deve dar o seu consentimento para a utilização dos dados pessoais, demonstrando que a empresa tem acesso a um vasto número de informações, bem como à câmera e ao microfone do próprio equipamento, contexto em que surge um pertinente questionamento: o que a empresa faz com tais dados pessoais? No caso do *Facebook*, são coletados diferentes tipos de informação dos usuários, a exemplo das pessoas e grupos com os quais eles se conectam. É possível inferir até mesmo o estado emocional das pessoas - por meio dos ícones de expressão (*emoticons*),

ao responder à rede social como está se sentindo (animado, cansado, feliz, dentre outros) ou ao emitir uma opinião sobre determinado assunto -, que acabam fornecendo um rico retrato de si (BIONI, 2019).

É preciso, porém, ir mais além quando se trata de vigilância sobre os indivíduos. Para além do monitoramento dos hábitos de navegação, a Internet juntamente com a tecnologia móvel permitiu o avanço, sem precedentes, da conexão dos indivíduos à rede. Assim, a onipresença da Internet possibilitou a verificação da localização geográfica (*global positioning system*/*GPS*) dos *smartphones*, possibilitando, por exemplo, que as publicidades sejam direcionadas com base nessa informação. No mundo globalizado, os dados de geolocalização são extremamente valiosos, sendo um dos motivos da aquisição do aplicativo *Waze* - que captura a localização dos seus usuários - pelo *Google*, na expressiva quantia de 1,3 bilhões de dólares (BIONI, 2019). Os dados são a nova moeda da economia, sendo inegável o fato de que empresas de tecnologia "são compradas e vendidas levando em consideração o seu patrimônio de base de dados" (PINHEIRO, 2018, p. 213), vide os exemplos acima delineados.

O breve panorama histórico traçado até então nos mostra como a privacidade dos indivíduos é constantemente violada e mitigada diante do aparecimento de novas tecnologias que possibilitam a sua permanente vigilância e monitoramento. Dessa forma, como bem nos assegura Laura Mendes,

> Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade. (2014, n.p.)

Portanto, neste capítulo inaugural, pretendeu-se examinar as principais características da atual sociedade da informação, bem como os novos desafios decorrentes dos avanços tecnológicos ocorridos dentro da história da humanidade. Delineadas essas considerações, faz-se necessário analisar o que são dados pessoais, como surgiu a coleta de dados, as espécies de dados e as principais normas relacionadas ao tema.

3 DOS DADOS PESSOAIS

Atribui-se aos dados pessoais papel de grande destaque na atual era tecnológica, e não sem razão, já que passaram a ser tratados sob uma nova perspectiva desde a evolução da informática e das telecomunicações. Devido a isso, o estudo do tema é de extrema relevância, uma vez que "todos os âmbitos da vida estão marcados pelo tratamento de dados pessoais" (MENDES, 2019, p. 1). Assim, partindo da ideia de que o fluxo internacional de dados é elemento fundamental para a atual economia globalizada (VAINZOF, 2019), far-se-á uma análise dos conceitos, espécies, princípios, bem como das principais normas, nacionais e internacionais, responsáveis pela proteção dos direitos dos indivíduos.

3.1 CONCEITOS, ESPÉCIES E PRINCÍPIOS RELACIONADOS AO TRATAMENTO DE DADOS

De início, faz-se necessário fazer uma diferenciação comumente trazida pela doutrina. Informações e dados são conceitos que não se equivalem, ainda que, muitas vezes, tratados como sinônimos. Dessa forma, pode-se dizer que o dado é um estado primitivo da informação (DONEDA, 2006), uma vez que sozinho não agrega conhecimento. O dado, portanto, está “associado a uma espécie de ‘pré-informação’, anterior à interpretação e ao processo de elaboração” (DONEDA, 2011). São fatos brutos, devendo ser organizados e processados para que, então, se tornem algo inteligível (BIONI, 2019). Assim,

> Tome-se, novamente, o exemplo citado da multinacional Zara [...][4]. A simples ação de coletar e acumular os fatos (dados) das vendas e saídas de seus produtos é algo que em si não é dotado de nenhum significado. Somente quando organizados, especialmente para o fim de identificar quais produtos foram os mais vendidos, extrai-se, então, uma informação útil. Especificamente, quais produtos tiveram melhor aceitação pelo mercado consumidor para (re)projetá-los de acordo com tal tendência. (BIONI, 2019, p. 36-37).

[4] A multinacional Zara, do segmento de vestuário, possui como uma de suas principais atividades o processamento de dados. “Os seus lojistas registram os dados das vendas, compartilhando-os com o centro de criação da marca em La Coruña. Uma vez constatada a reação do mercado, isto é, quais itens foram mais aceitos pelos consumidores, os produtos são (re)projetados com base em tal padrão de consumo. Somente após tal retroalimentação, inicia-se, novamente, o processo de produção do bem de consumo”. (BIONI, 2019, p. 10).

Nesse contexto, é imprescindível o gerenciamento de um banco de dados, de forma manual ou automatizada, para que deles seja extraído uma informação útil capaz de agregar conhecimento que possa ser revertido para a tomada de uma decisão (BIONI, 2019). Superada tal questão, cumpre mencionar que o Brasil adotou o conceito expansionista de “dado pessoal”, sendo esse referente a uma pessoa identificada ou identificável.

Ademais, segundo a Lei Geral de Proteção de Dados brasileira, os dados podem ser: diretos, quando identificam diretamente uma pessoa natural, sendo desnecessárias outras informações para tanto, como CPF, RG, nome e título eleitoral, e indiretos, responsáveis por tornar a pessoa natural identificável, uma vez que necessitam de informações adicionais para identificá-la, como gostos, hábitos, interesses de consumo, profissão, sexo, idade e geolocalização. Quando o seu tratamento puder trazer algum tipo de discriminação e implicar riscos e vulnerabilidades aos direitos e liberdades fundamentais dos titulares, temos os dados chamados sensíveis, relativos à origem racial, convicção religiosa, opinião política, dados referentes à saúde, dentre outros (VAINZOF, 2019).

Ainda, existem os dados pseudonimizados, referentes àqueles que perdem a possibilidade de associação, direta ou indireta, a certo indivíduo. Assim, só poderão ser associados a uma pessoa em específico caso existam informações adicionais que possam ser utilizadas. Por fim, os dados anonimizados não são considerados dados pessoais, já que se referem a titulares não identificáveis, ainda que utilizados meios técnicos razoáveis e disponíveis quando do seu tratamento (BRASIL, 2018).

Frise-se que o “dado anônimo” é justamente o contrário de “dado pessoal”, visto que incapaz de revelar a identidade de uma pessoa. Pelo próprio significado do termo, anônimo é aquele que não possui nome nem rosto (BIONI, 2019). Dessa forma, o processo pelo qual é desfeito o vínculo entre o dado e o seu respectivo titular é denominado “anonimização”, trazendo a LGPD que:

> Art 5º Para os fins desta Lei, considera-se
> [...]
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo. (BRASIL, 2018)

Trata-se de processo que elimina a *identificabilidade* dos dados (BIONI, 2019), devendo ser aplicado, sempre que possível, quando do seu processamento

pelos agentes de tratamento. Assim, dados desnecessários, excessivos, ou tratados em desconformidade com a lei podem ser anonimizados, buscando-se, com tal ação, a preservação de direitos fundamentais dos titulares.

Diversas normas que versam acerca do tratamento de dados trazem uma série de princípios correlatos, existindo um verdadeiro núcleo comum que ficou conhecido como *Fair Information Practice Principles (FIPPs)*, que formam a espinha dorsal de inúmeros regramentos existentes atualmente. Tanto o Regulamento Europeu quanto a Lei Geral de Proteção de Dados brasileira, por exemplo, trataram do tema de forma autoexplicativa e elencaram normas principiológicas que servem de verdadeiro norte para os agentes de tratamento.

Dessa forma, a LGPD, de forma extremamente clara e precisa, dispõe, *in verbis:*

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

Considerando a clareza da norma ora estudada, o presente trabalho não se deterá, de forma mais detalhada, sobre todos os princípios aqui elencados. Tem-se que esses representam limitações ao tratamento de dados, buscando empoderar o

titular de forma a aumentar suas chances de controle, decidir acerca do fluxo de seus dados pessoais e propiciar a autodeterminação informativa (VAINZOF, 2018). Nesse sentido, o reconhecimento da proteção de dados como direito fundamental autônomo oportunizaria a maior efetivação dessas normas principiológicas e dos valores que elas carregam.

3.2 HISTÓRICO REGULATÓRIO DA PROTEÇÃO DE DADOS

A origem da regulamentação referente à proteção de dados pode ser facilmente remetida à segunda metade do século XX. O contexto histórico aponta que, após a Segunda Guerra Mundial, diversos governos perceberam que as informações pessoais de seus cidadãos eram extremamente úteis para planejar e coordenar um crescimento ordenado (BIONI, 2019, p. 113). Não restam dúvidas de que foi a tecnologia que viabilizou essa nova faceta do Estado, resultando na criação de diversos bancos de dados e no aumento da capacidade de processamento das mais variadas informações.

Assim, os marcos regulatórios subjacentes à proteção de dados pessoais estão originalmente ligados ao direito da privacidade. A utilização de novos aparatos tecnológicos para acessar e divulgar fatos relativos à esfera privada dos indivíduos gerou intenso debate doutrinário acerca da matéria, destacando-se o pioneiro artigo, datado de 1890, dos norte-americanos Samuel Warren e Louis Brandeis, denominado "The Right to Privacy". Os renomados autores denunciaram, assim, a intensa violação da vida privada e doméstica dos indivíduos pela imprensa bem como defenderam a necessidade de reconhecimento, pelas cortes americanas, do direito a ser deixado só (MENDES, 2014). Já nessa época, propuseram o direito dos indivíduos de estarem só com seus pensamentos, emoções e sentimentos, independentemente da forma de expressão (VIEIRA T., 2007, p. 33), revertendo-se de particular importância o rompimento com a tradição patrimonialista que associava a proteção da vida privada à propriedade.

A partir da análise do supracitado artigo, percebe-se que o direito à privacidade teve, em seus primórdios, um caráter iminentemente individualista, em que sobressaíam as suas características de direito negativo. Dessa maneira, para a sua efetiva garantia, era exigida a total abstenção do Estado na esfera privada dos

indivíduos, vez que, sem privacidade, "não há condições propícias para o desenvolvimento livre da personalidade" (MENDES, BRANCO, 2015, p. 280). Assim, os autores concluíram, analisando diversos precedentes judiciais da Suprema Corte dos Estados Unidos, que se poderia extrair de tais decisões um direito geral à privacidade, desvinculado do direito à propriedade privada e com características de direito pessoal.

Com a revolução tecnológica aliada à transformação da função do Estado, houve uma mudança significativa no alcance bem como no sentido do direito à privacidade. Assim, de um direito com dimensão negativa, quase egoísta, passou a ser considerada uma garantia do indivíduo para controlar suas próprias informações bem como pressuposto para todo e qualquer regime democrático. Não restam dúvidas de que, hoje, o direito à privacidade adquiriu um caráter eminentemente positivo, demandando do Estado não mais uma abstenção geral, mas, sim, ações para a sua efetiva concretização. Dessa forma, transformou-se para incluir a dimensão de proteção de dados pessoais, devido ao tratamento informatizado de dados e ao intenso fluxo de informações (MENDES, 2014).

Nesse contexto, com bem nos assegura Danilo Doneda (2006), o direito à privacidade apresentou caráter individualista durante longo tempo, e a sua inserção em ordenamentos de cunho patrimonialista fez com que tal garantia se estendesse apenas a indivíduos pertencentes a classes sociais bem determinadas, acarretando certo "elitismo" nos tribunais. Afirma o autor que tal tendência foi relativizada a partir da década de 60, época relacionada ao panorama do *welfare state*, à mudança do relacionamento entre Estado e cidadão, ao aumento da capacidade técnica para recolher, processar e utilizar a informação bem como às maiores reivindicações por mais direitos pelo povo. Sob essa ótica, as informações pessoais ganham particular relevância, constatando-se que não mais apenas figuras de grande relevo social possuíam a sua privacidade violada, mas também grande parte da população.

Assim, diante da perspectiva de que o desenvolvimento tecnológico deve ser harmonizado com a privacidade dos cidadãos, o direito à privacidade se reinventou para abarcar a disciplina da proteção de dados pessoais. Ambas partilham dos mesmos fundamentos: a tutela da personalidade e da dignidade do indivíduo, porém com feição própria. Essa proteção é ainda mais relevante quando se considera a atual sociedade da informação, caracterizada essencialmente por relações remotas,

virtuais, em que os dados pessoais se constituem na única forma de representação das pessoas perante organizações estatais e privadas (MENDES, 2014). Torna-se, portanto, de fundamental importância à análise da tutela jurídica dos dados pessoais, para melhor compreender como diversos países trataram do tema no decorrer das últimas décadas.

3.2.1 Previsão Normativa Internacional

Reverte-se de particular importância à análise das gerações de leis de proteção de dados pessoais proposta por Viktor Mayer-Schonberger, que nos oferece uma compreensão histórico-evolutiva acerca do tema (MENDES, 2014). A primeira geração de leis de proteção de dados pessoais surgiu na década de 70, como principal reação ao processamento eletrônico de dados realizado pelo Estado. Temia-se o surgimento da figura *orwelliana* do Grande Irmão, que poderia sufocar a liberdade do indivíduo, mediante uma vigilância ostensiva (BIONI, 2019). Assim, a saída foi domesticar e regular a própria tecnologia, que deveria ser orientada por valores democráticos, bem como controlar a criação dos bancos de dados através de concessões e autorizações para o seu funcionamento (DONEDA, 2006). Podem-se citar, como exemplo de normas de primeira geração, devido a sua estrutura e linguagem, "as leis do Estado alemão de Hesse (1970), a Lei da Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977)" (MENDES, 2014).

O advento do Estado Social requeria, para o seu pleno funcionamento, a coleta e o processamento dos dados dos seus cidadãos, citando-se como exemplo as propostas feitas pelo Parlamento da Suécia, em 1960, de fundir todas as informações fiscais, de registro e dados do censo em um único banco de dados, bem como o Comitê alemão criado pelo governo para interligar dados municipais, estaduais e federal. Nos Estados Unidos, cabe apontar o famoso caso do "*National Data Center*" proposto pelo governo em 1965, mas que nunca saiu do papel. O plano era a criação de um banco de dados nacional centralizado com o objetivo de reduzir custos, uma vez que os demais órgãos do governo não precisariam investir

em tecnologia de armazenamento e informática (MENDES, 2014). Nesse sentido, como bem nos ensina Laura Mendes,

> À medida que o projeto evoluiu, chegou-se à ideia que o centro deveria conter dados de todos os cidadãos americanos em relação a data de nascimento, cidadania, registros escolares, serviço militar, registros de impostos, benefícios da previdência social, registro do espólio, e, eventualmente, registros criminais. Procederam-se a inúmeras discussões nos meios de comunicação e a diversas audiências no Congresso. Esses debates culminaram em um debate público acerca dos potenciais danos que tal centralização de dados poderia causar, principalmente em razão do grande poder que ele conferia ao Estado sobre a vida de todos os cidadãos, ameaçando gravemente a tradição liberal americana. Assim, o "National Data Center" nunca chegou a ser construído. (MENDES, 2014, n.p.)[5]

Posteriormente, o processamento de dados transcendeu a esfera governamental, o que demandou uma nova estrutura normativa, fazendo surgir a segunda geração de leis. Dessa forma, ocorreu uma proliferação dos bancos de dados, preocupando-se os cidadãos não apenas com as bases de dados estatais, mas também com as da esfera privada (DONEDA, 2006).

Aparecem, portanto, as figuras dos “Pequenos Irmãos”, bancos de dados existentes tanto no âmbito estatal quanto no âmbito privado[6] (RAMOS, 2011, p. 957) conectados em rede e espalhados por todo o mundo (MENDES, 2014). Abandona-se a estratégia regulatória anterior, que atribuía ao Estado licenciar a criação de todos os bancos de dados, para transferir ao próprio titular a responsabilidade de protegê-los. Nesse contexto, se o fluxo das informações era autorizado pelo Estado, agora o próprio cidadão deve possuir tal responsabilidade, por meio do seu consentimento (BIONI, 2019).

A terceira geração de leis de proteção de dados pessoais tem seu marco inicial com a decisão do Tribunal Constitucional alemão, em 1983, que declarou parcialmente inconstitucional a Lei do Censo (vide subcapítulo 3.1). O Tribunal, ao reinterpretar a Lei Federal de Proteção de Dados Pessoais alemã à luz da Lei

---

[5] Ainda segundo a autora, "Como se vê, a reação dos cidadãos contra as tentativas dos governos de utilizar a tecnologia existente para ampliar a coleta e o processamento de dados foi extremamente forte, dado o temor do poder de controle de uma burocracia automatizada e desumanizada. A reivindicação da opinião pública voltava-se prioritariamente no sentido de se controlar a tecnologia, o que acabou por influenciar as legislações de proteção de dados. Grande parte das leis da década de 70 tem uma perspectiva funcional e buscar controlar os bancos de dados de forma *ex ante*, condicionando o seu funcionamento à licença prévia ou ao registro nos órgãos competentes. Ademais, ao priorizar o controle rígido dos procedimentos, as normas desse período deixavam para segundo plano a garantia do direito individual à privacidade, o que pode ser percebido a partir do próprio jargão técnico utilizado pelas normas.” (2014 n.p.)

[6] “Chamaram esses bancos de dados de “Pequeno Irmão”, alusão ao Grande Irmão orwelliano. [...] Como veremos, necessitamos de amarras ao “Pequeno Irmão”, que possui mais dados sobre os brasileiros que o próprio Poder Público” (RAMOS, 2011, p. 957-959).

Fundamental de Bonn, declarou que os cidadãos possuem direito à autodeterminação informativa e sua participação passa a ser assegurada em todo o processamento de seus dados, desde a coleta até o compartilhamento, e não apenas como uma opção entre “tudo ou nada” (MENDES, 2014). São exemplos de leis da terceira geração,

> (...) as leis dos Estados alemães após a decisão do Tribunal Constitucional, a emenda à Lei Federal de Proteção de Dados Pessoais de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda. (MENDES, 2014, p. x)

A quarta geração de leis veio para resolver certos problemas apresentados nos períodos anteriores - como a falta da efetiva participação do indivíduo no controle dos seus dados -, fortalecendo o papel do cidadão e o seu autocontrole sobre os dados pessoais. As normas não deixaram no âmbito de escolha do indivíduo o processamento de determinados dados, por entenderem que são tão relevantes para o indivíduo que merecem uma proteção especial: são os dados considerados sensíveis. Como visto, dizem respeito à etnia, religião, opção sexual, opinião política e a outras informações capazes de gerar discriminação, e que não devem estar no âmbito de disposição do indivíduo.

Outra característica refere-se à adoção, em diversos países, de leis gerais complementadas com normas setoriais, com o propósito de aumentar a proteção do indivíduo nos mais variados âmbitos em que existe o tratamento de dados. Assim, a legislação acaba por contemplar as mais variadas especificidades existentes (MENDES, 2014). Ademais, houve a disseminação de autoridades administrativas competentes para a aplicação das leis, o que aumentou significativamente o âmbito de proteção. O consentimento, por sua vez, passou a ser adjetivado como "livre, informado, inequívoco, explícito e ou/específico" (MAYER-SCHONBERGER *apud* BIONI, 2019, p. 117), tornando-se vetor central quando da discussão acerca do tema.

Tal desenvolvimento geracional pode ser analisado nas *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Tal organismo internacional multilateral possui a missão de promover o bem-estar econômico e social global, tendo sido criado após a Segunda Guerra Mundial, em 1948. Assim, possui o objetivo de estabelecer, entre seus países-membros, uma relação de cooperação para solucionar problemas comuns que os afligem, visando a

estabelecer padrões que gerem respostas uniformes (BIONI, 2019). Nesse contexto, percebeu-se, por volta de 1980, que o desenvolvimento econômico e social havia se voltado à tecnologia da informação, existindo um intenso fluxo de processamento dos dados pessoais dos cidadãos, fazendo-se necessário conciliar tal cenário com a privacidade dos indivíduos.

A OCDE, portanto, emitiu dois documentos que influenciaram mundialmente a proteção de dados: *privacy guidelines*, em 1980, e *declaration on transborder data flows*, em 1985. Fica claro que o "resultado desejado era criar um *ambiente regulatório uniforme* entre os países-membros e, ante a inexistência de disparidades regulatórias, garantir o livre trânsito das informações" (BIONI, 2019, p. 119). Pode-se dizer que tais diretrizes, por estabelecerem que o cidadão deve possuir controle sobre os seus dados pessoais, situam-se entre a terceira e quarta geração de leis.

O direito comunitário europeu foi pioneiro quanto à matéria de proteção de dados pessoais. Sem pretender esgotar a matéria, analisaremos algumas Convenções e Diretivas, assim como a *General Data Protection Regulation* (GDPR), grande influenciadora da Lei Geral de Proteção de Dados brasileira (LGPD).

A primeira que merece destaque é a Convenção 108, aprovada pelo Conselho da Europa, em Estrasburgo na década de 1980, podendo-se afirmar que,

> "(...) foi o primeiro texto jurídico unificado sobre a matéria, que se propôs a garantir, no território de cada país-membro, o respeito aos direitos e liberdades fundamentais de todas as pessoas, independentemente de suas nacionalidades ou residências, atendendo, também, à proteção do tratamento automatizado de dados pessoais" (RUARO, RODRIGUEZ, 2010, p. 167).

Recebeu a denominação de "Convenção para Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal" bem como estabeleceu uma proteção mínima para a proteção de dados pessoais, não impedindo que Estados signatários elevassem tal proteção (MARQUES, MARTINS, 2006). Ademais, representou grande avanço ao admitir como signatários países não europeus (VIEIRA T., 2007). Em que pese o avanço conferido por tal Convenção, a ratificação por poucos Estados-membros e seu o caráter *non self-executing* - que a fazia depender de legislações nacionais específicas para sua aplicação, as quais nem sempre existentes - tornaram-se obstáculos para a sua eficácia (MARQUES, MARTINS, 2006).

Posteriormente, visando a resolver tais problemas, foi aprovada a Diretiva 95/46/CE da União Europeia, com o objetivo de aperfeiçoar as diretivas da OCDE e da Convenção 108. Assim,

> (...) os objetivos principais da edição da Directiva, além da atualização tecnológica, centravam-se na harmonização de toda a legislação vigente na Europa sobre proteção de dados pessoais, a fim de facilitar o fluxo internacional dessas informações no mercado interno, e reforçar as medidas e procedimentos de segurança durante o tratamento dos dados pessoais, especialmente no que concerne aos serviços de telecomunicações e de correio eletrônico. (VIEIRA T., 2007, p. 236).

Nesse contexto, um dos principais motivos para a sua edição foi justamente a falta de homogeneidade da legislação europeia, que possuía diferentes regulamentações para o processamento e transmissão de dados entre os Estados-membros. Dentre as suas principais características, destaca-se a admissão apenas de países europeus e a obrigação dos Estados-membros de adotarem as disposições legislativas necessárias para dar cumprimento a Diretiva, respeitando-se o prazo de 3 anos para tanto, conforme preceitua o item 1 do art. 32º[7] (VIEIRA T., 2007, p. 237).

Cumpre salientar, ainda, que:

> Na UE, a questão da proteção de dados pessoais encontra-se em fase tão avançada que, após a incorporação da Directiva 95/46/CE ao ordenamento jurídico dos diversos Estados-membros, iniciou-se o controle pela via administrativa. Hoje, todos os países da Europa dispõem de uma agência, de uma comissão ou, pelo menos, de um departamento, nos respectivos governos, responsável pela proteção de dados pessoais e pela fiscalização da aplicabilidade da Directiva (...). (VIEIRA T., 2007, p. 238).

Ademais, a Diretiva trouxe diversos princípios a serem observados pelos países-membros, citando-se, como exemplo, os princípios da lealdade ou boa-fé, publicidade, transparência, proporcionalidade, veracidade, confidencialidade, dentre outros. Além disso, estabeleceu que a proteção de dados deveria ser aplicada tanto no tratamento manual quanto no tratamento automatizado de dados, devendo ser observada pelo setor público e privado (RUAREZ, RODRIGUEZ, 2010). Outras duas diretivas merecem ser mencionadas, quais sejam, a Diretiva 97/66/CE, de 1997, que tem por objetivo regular a proteção da intimidade na área das telecomunicações, bem como a Diretiva 2002/58/CE, de 2002, responsável por tratar acerca da

[7] Artigo 32º 1. Os Estados-membros porão em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento a presente directiva o mais tardar três anos a contar da data da sua adopção" (UNIÃO EUROPEIA, 1995).

proteção da privacidade no setor de comunicações eletrônicas, especialmente em razão do avanço tecnológico sem precedentes (PEZZI, 2007, p. 101).

Posteriormente, destaca-se a Diretiva 2006/24/CE, que regulamenta a conservação de dados gerados ou tratados no âmbito da oferta de serviços de comunicações eletrônicas. Tal normativa prevê, por exemplo, que os dados poderão ser transmitidos às autoridades nacionais em casos específicos e de acordo com a legislação nacional, estabelecendo, ainda, que determinados dados sejam disponibilizados para investigação, detecção e repressão de crimes graves, pelo prazo máximo de 24 meses (RUAREZ, RODRIGUEZ, 2010).

Faz-se necessário, por fim, tecer comentários acerca da *General Data Protection Regulation* (GDPR) ou Regulamento Geral de Proteção de Dados (RGPD), que revogou a Diretiva 95/46 e tornou-se reconhecida mundialmente devido a sua robustez e importância. Assim, a adoção de um Regulamento Geral fez da União Europeia modelo internacional no que se refere à proteção de dados, sendo o GDPR a mais avançada e rigorosa norma sobre a matéria.

O foco da norma é a proteção dos direitos e garantias fundamentais dos cidadãos quando do tratamento de dados, de modo a propiciar aos titulares dos dados integral controle e entendimento sobre o que está sendo realizado com suas informações pessoais. A aplicação do Regulamento se dá, portanto, de maneira uniforme nos 28 países membros da União Europeia e, ainda, em três países do Espaço Econômico Europeu (Noruega, Islândia e Liechtenstein), sendo mais eficaz quando comparado com a Diretiva 95/46, a qual demandava a criação de leis internas em cada país-membro, nem sempre existentes, para que se tornasse válida na prática (LIMA, 2018).

Frise-se que o GPDR passou a ter eficácia plena em 25/05/2018, após dois anos de *vacatio legis*, e será aplicado independentemente da nacionalidade do indivíduo e do local de sua residência. Ou seja, pode o Regulamento ser aplicado a titulares de outras cidadanias, não sendo relevante saber se está diante de cidadão europeu ou não, assim como poderá ser aplicado para os cidadãos que apenas estejam em trânsito no território da União Europeia (LIMA, 2018).

Quanto à aplicação material do GDPR, o seu artigo 2º (1) estabelece quais atividades estão abarcadas no Regulamento, sendo elas "o tratamento de dados pessoais por meios total ou parcialmente automatizados" assim como o "tratamento

por meios não automatizados de dados pessoais contidos em arquivos ou que visem à formação de arquivo" (LIMA, 2018. p. 26). Assim, pode-se dizer que o GDPR é "tecnologicamente neutro", uma vez que não se limita ao tratamento de dados por meio automatizados, aplicando-se também ao tratamento manual. Ademais, por se tratar de Lei Geral, contempla diversas relações possuindo ampla aplicabilidade, as quais se incluem as relações de consumo, relações de emprego, interações por meio da *internet*, tratamento de dados de crianças e adolescentes, dentre outros (LIMA, 2018).

Em relação à aplicação territorial, consta do artigo 3º (1) do GDPR que o mesmo será aplicado a estabelecimentos situados no território da União, tratando-se de critério baseado na localização física do estabelecimento. Dessa forma, o Regulamento se aplica às empresas que possuem sede na União Europeia, ainda que o tratamento e armazenamento de dados aconteçam fora do território (UNIÃO EUROPEIA, 2018).

Cabe apontar que o artigo 4º do GDPR estabelece uma série de definições relevantes como, por exemplo, as definições de dado pessoal, dado genético, biométrico, relativos à saúde e dados sensíveis. O artigo 5º, à semelhança de outras normas europeias, traz uma série de princípios relativos ao tratamento de dados, como os da licitude, lealdade, transparência, limitação da finalidade, minimização dos dados, limitação da conservação, exatidão, integridade e confidencialidade. Nesse contexto, o tratamento de dados somente será permitido se considerar tais princípios bem como será considerado lícito se atender a pelo menos uma das seguintes hipóteses legais taxativas, previstas artigo 6º, item 1 da GDPR:

> a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
> b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
> c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
> d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
> e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
> f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

É de crucial importância, portanto, que os responsáveis pelo tratamento dos dados avaliem os propósitos específicos que almejam desde a concepção do projeto que envolva a coleta de dados, uma vez que servirão como uma fronteira de legalidade para o seu uso (VAINZOF, 2018). Em seu artigo 4º, item 7, o Regulamento traz a definição de "responsável pelo tratamento" sendo aquela "pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais" (UNIÃO EUROPEIA, 2018). Por conseguinte, os termos "finalidades" e "meios de tratamento" "estão relacionados ao nível de influência do agente em definir o *porquê* e o *como* os dados serão tratados" (CHAVES, 2018, p. 114). Internacionalmente, o responsável pelo tratamento é conhecido por *controller*, sendo tal expressão comumente utilizada pela doutrina nacional.

Mais adiante, o GDPR, em seu artigo 4º item 8, traz a importante definição de "subcontratante", que seria a "pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes" (UNIÃO EUROPEIA, 2018). Assim, o subcontratante depende do responsável pelo tratamento de dados para que possa ser caracterizado em um determinado contexto, estando o seu conceito intimamente ligado com a ideia de delegação (CHAVES, 2018). O subcontratante é conhecido como *processor* e está limitado às delegações que lhe foram atribuídas pelo *controller*, possuindo "certa liberdade para definição dos *meios* de tratamento de dados pessoais (mas não finalidades), mediante autorização tácita ou expressa do responsável." (CHAVES, 2018, p. 116).

O Regulamento traz, ainda, conceitos relevantes como *privacy by design* e *privacy by default*[8], com o intuito de encorajar empresas que concebem produtos e serviços a incorporar a privacidade em todos os projetos de tecnologia. Dessa forma, partindo da ideia de que apenas leis não serão suficientes para garantir a privacidade dos usuários, o GDPR adota tais metodologias que deverão ser observadas pelas mais variadas empresas, de modo a proteger o usuário desde a concepção de quaisquer sistemas de tecnologia da informação. A privacidade é, então, incorporada à própria arquitetura técnica dos produtos ou serviços, devendo

[8] Termos que se referem a “privacidade por design” e “privacidade por padrão” (*Tradução nossa*).

os sistemas, por configuração padrão, garantir a proteção dos dados pessoais (JIMENE, 2018). Tal tendência foi refletida no cenário brasileiro a partir da Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 46, parágrafo 2º, ao afirmar que "As medidas de que trata o *caput* deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução" (BRASIL, 2018).

Frise-se que o GDPR estabelece a necessidade de criação de autoridades para proteção de dados ("DPAs" – *Data Protection Authorities*), públicas e independentes, em cada Estado-membro, para aplicação e fiscalização do Regulamento. É o que se depreende da leitura do artigo 51, que ressalta a importância das autoridades na defesa dos direitos e liberdades fundamentais dos indivíduos, no que concerne ao tratamento de dados, além de atuar na facilitação da circulação desses dados na União. Além disso, as autoridades devem agir sem qualquer tipo de influência externa, com total independência, para que, com isso, consigam alcançar os seus objetivos e executar suas atribuições (art. 52).

Dentre as atribuições de cada autoridade, em seu artigo 57, o GDPR estabelece que a elas cabe a execução do Regulamento; a conscientização do público em geral quanto à regras e direitos previstos no GDPR; o aconselhamento do Governo e do Parlamento nacional no que tange ao respeito de medidas legislativas e administrativas; a prestação de informações aos titulares dos dados bem como a análise de suas reclamações; a investigação de ilícitos; a orientação acerca dos das operações de tratamento, dentre outros. Nesse contexto,

> Observa-se que a competência e atribuição das DPAs excedem a mera investigação de casos, e se pauta pela conscientização da sociedade em geral sobre as melhores normas aplicáveis aos tratamentos de dados e as implicações da questão no mundo contemporâneo (BLUM, ARANTES, 2018, p. 239).

Verifica-se, ainda, que as DPAs possuem poderes investigativos - requerer informações, documentos, acessos à instalações daqueles que tratam os dados, entre outros -, corretivos - fazer advertências, retirar certificações, ordenar ao responsável de tratamento que comunique ao titular a violação dos seus dados -, e consultivos - relacionados à conscientização da sociedade acerca da importância do Regulamento -, elencados no artigo 58. Na sequência, o GDPR prevê a aplicação de vultosas multas nos casos de violação às suas disposições, estabelecendo o artigo 83 as condições gerais para aplicação das sanções pecuniárias como, por exemplo,

natureza da gravidade, número de titulares afetados, a duração da infração, a reincidência dos infratores, dentre outros. Destaca-se, portanto, o papel dissuasório e educativo das multas, que podem chegar ao patamar de 20 milhões de euros (BLUM, ARANTES, 2018, p. 250).

Ademais, conforme as Considerandas 1 e 2 do Regulamento, a "proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental", possuindo o GDPR o "objetivo de contribuir para a realização de um espaço de liberdade, segurança e justiça" assim como de união econômica e social, visando o bem-estar das pessoas singulares (UNIÃO EUROPEIA, 2018).

Por fim, vale a pena discorrer acerca da importância do GDPR para o desenvolvimento econômico da União Europeia. Isso porque, muitas das críticas ao Regulamento europeu referem-se à possibilidade da novel lei trazer impactos negativos à economia por representar um obstáculo ao desenvolvimento de negócios e empresas que dependem dos dados pessoais para o seu bom funcionamento. Caio César Carvalho Lima elucida bem a questão, ao afirmar que:

> (...) a proteção de dados tem que ser levada a sério, a fim de que isso traga a confiança necessária a todos os atores de mercado, tanto da esfera pública quanto privada, facilitando a troca de dados, ao mesmo tempo que propicie que negócios se desenvolvam, diante da economia digital. Portanto, **a criação de uma Lei Geral pode servir para consolidar determinada nação como "porto seguro" de investimento, na medida em que se conseguirá ter clara dimensão sobre os limites do que é permitido, proibido, quais são as responsabilidades e os riscos, além das sanções a que estarão sujeitos, no caso de descumprimento da legislação. Com isso, mais investimentos acontecerão, não apenas internos, mas também externos, diante da segurança jurídica que será alcançada.** (2018, p. 25, *Grifo nosso*)

Delineados os principais marcos regulatórios que elevaram a União Europeia ao principal patamar no que se refere à proteção de dados, passaremos a analisar as principais normais nacionais relativas ao tema, tecendo maiores detalhes, dentre elas, à nova Lei Geral de Proteção de Dados (13.709/2018), que entrará plenamente em vigor em agosto de 2020.

3.2.2 Previsão Normativa Brasileira

Primeiramente, cumpre ressaltar que a proteção de dados no Brasil igualmente se iniciou a partir de uma evolução do conceito de privacidade, podendo-se afirmar que houve um amadurecimento natural de tal direito

fundamental diante da nova realidade imposta pela sociedade da informação. Destacamos, ainda, que não é mais suficiente interpretá-lo como o *direito de estar só*, como anteriormente mencionado, devendo ser necessariamente considerado, dentro do seu espectro, o direito à autodeterminação informacional.

Dessa forma, os indivíduos possuem direitos sobre suas informações pessoais, contidas nos mais variados bancos de dados, que envolvem a determinação de como tais informações serão utilizadas e como essa esfera privada será construída (RODOTÀ, 2008). Analisar-se-ão, portanto, as principais normas que regulam a privacidade e a proteção de dados pessoais no ordenamento jurídico nacional.

3.2.2.1 Constituição da República (CRFB/88)

Pode-se dizer que a Constituição brasileira, em sua redação original, protege os dados pessoais de forma indireta. A CRFB/88 estabelece, em seu artigo 5º inciso X, que são invioláveis a intimidade, a privacidade, a honra e a imagem das pessoas e, em caso de violação desses direitos, assegura o direito à indenização pelo dano material ou moral sofrido (BRASIL, 1988). Mais adiante, no inciso XII, prevê acerca da inviolabilidade da correspondência, das comunicações telegráficas, *de dados* – menção essa explicitada no terceiro capítulo do presente trabalho - e das comunicações telefônicas. Resguarda, ainda, em seu inciso XXXIII, o direito de todos de receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, ressalvadas as sigilosas, imprescindíveis para a segurança do Estado, bem como regula o *habeas* data no inciso LXXII, para assegurar o conhecimento e retificação de dados pessoais relativos à pessoa do impetrante.

O *habeas data* foi regulamentado no plano infraconstitucional pela Lei nº 9.507/1997. Conceder-se-á *habeas data*, portanto, para assegurar o direito líquido e certo do impetrante ao conhecimento de informações relativas à sua pessoa, constantes de registros ou banco de dados de entidades governamentais ou de caráter público; a retificação de dados bem como a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro justificável e que esteja sob pendência judicial ou amigável, consoante preceitua os artigos 5º, LXXII

da CRFB/88 e 7º da Lei 9.507/1997 (BRASIL, 1988, 1997) Nesse contexto, considera-se de caráter público todo registro ou banco de dados contendo informações que sejam, ou possam ser, transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações (art. 1º, parágrafo único, da Lei 9.507/1997).

Vislumbra-se, assim, que tal ação adveio em um contexto de pós-regime ditatorial, em que existia a necessidade de um instrumento que possibilitasse a requisição de informações pessoais perante a administração pública visando à proteção de direitos fundamentais assim como a formação de uma cultura democrática (DONEDA, 2006). A privacidade, então, é protegida no seu viés da autodeterminação informacional, já que o titular dos dados possui acesso às suas informações pessoais presentes em bancos de dados públicos, podendo retificá-las, o que demonstra o seu controle sobre elas (DONEDA, 2006).

3.2.2.2 Código de Defesa do Consumidor

A Lei 8.078/90 foi a primeira que tratou do tema de forma atual, objetivando lidar com as novas tecnologias de processamento de dados (MENDES, 2014). Assim, regula os bancos de dados e os cadastros dos consumidores e, em seu artigo 43, estabelece que o consumidor terá acesso às informações constantes em fichas, cadastros, registros bem como a dados pessoais e de consumo a que ele se refiram (BRASIL, 1990). Ademais, podemos afirmar que o papel de destaque dos arquivos de consumo deve-se, principalmente, aos bancos de dados de controle de crédito como, por exemplo, o SPC[9] e o SERASA[10], os quais, "em razão da massificação das relações comerciais, buscaram superar o anonimato dos partícipes dessa relação" gerenciando informações que determinarão o grau de confiabilidade e capacidade creditícia do consumidor. Tais arquivos, apesar dos inegáveis

[9] SPC: Serviço de Proteção ao Crédito. É ligado à Confederação Nacional dos Dirigentes Lojistas (CNDL) e está presente em todo o território nacional, por meio de mais de 2.200 entidades. Possui caráter público (§4º do art. 43 da Lei 8.078/90) e submetem-se às normas do Código de Defesa do Consumidor. Disponível em <https://www.spcbrasil.org.br/institucional/spc-brasil>. Acesso em: 15 nov. 2019.

[10] SERASA: é líder em serviços de informação, sendo responsável pela maior base de dados da América Latina. Desenvolvem soluções para reduzir riscos de crédito, evitar fraudes, vender a prazo com segurança, renegociar e recuperar dívidas, dentre outros. Possui uma média de 6 milhões de consultas diárias, ajudando consumidores, empreendedores e empresas de todos os portes e segmentos. Disponível em <https://www.serasaexperian.com.br/sobre>. Acesso em: 15 nov. 2019.

benefícios que trazem, devido a sua clareza, organização e facilidade de consulta, se utilizados de maneira indevida, podem violar diversos direitos constitucionais, como o da privacidade (PEZZI, 2007).

A amplitude do dispositivo demonstra a intenção do legislador de abarcar todo e qualquer dado pessoal do consumidor, não se limitando aos bancos de dados que possuem informações negativas para concessão de crédito (BESSA, 2010). Tal legislação, portanto, igualmente conferiu ao consumidor o direito de autodeterminação informacional, na tentativa de capacitá-lo para o controle das informações que lhe dizem respeito (BIONI, 2019).

Assim, devem ser atendidos diversos preceitos para que bancos de dados e cadastros de consumidores funcionem de forma plena, como, por exemplo: a possibilidade de acesso pelo consumidor às suas informações (direito de acesso); os dados arquivados devem ser claros, verdadeiros e objetivos, com linguagem de fácil compreensão (princípio da qualidade dos dados); o consumidor deve ser notificado acerca da abertura de um banco de dados pessoais quando por ele não solicitado (princípio da transparência); a obrigação dos bancos de dados de retificarem informações errôneas ou inexatas que dizem respeito aos consumidores (direito de retificação e cancelamento) e, por fim, para o armazenamento de informações negativas, deve ser observado o limite temporal de cinco anos (princípio do esquecimento). (MENDES, 2014).

Dessa forma, como bem nos assegura Bruno Bioni, tais direitos previstos no CDC gravitam em torno do consumidor, buscando, à semelhança das normas internacionais analisadas, conferir a ele uma posição de protagonismo em relação às suas próprias informações pessoais (BIONI, 2019).

3.2.2.3 Lei do Cadastro Positivo

A Lei n. 12.414/2011 disciplina, em seu art. 1º, a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou jurídicas, para formação de cadastro de crédito. Dessa forma, o consumidor não é analisado apenas por um viés "negativo", em relação as suas dívidas não pagas, mas, também, a partir de outras informações "positivas" que demonstram o seu histórico de adimplemento bem como a sua capacidade financeira (BESSA, 2011).

Após a edição de tal lei, tornou-se possível a divulgação das boas práticas comerciais da maioria dos consumidores, representando um avanço em direção à ética e ao prestígio da ideia de cumprimento das obrigações firmadas. Portanto, o cadastro de adimplemento se constitui em um conjunto de dados e informações diversas, que abarca o comportamento, a vida e o histórico de consumo do indivíduo, permitindo ao concedente de crédito analisar a vantagem ou não de concedê-lo (COSTA, 2012).

A LCP estabeleceu a orientação de que é direito do titular dos dados gerenciar as suas informações pessoais, requerendo, por exemplo, o consentimento expresso do titular dos dados pessoais por meio de assinatura em instrumento específico (art. 4º). Assim, estabeleceu mais do que a simples comunicação acerca da abertura do banco de dados, tal como fez o Código de Defesa do Consumidor (BIONI, 2019), incluindo, ainda, tal consentimento específico quando do compartilhamento da base de dados com terceiros (art. 9º).

Ademais, a referida peça legislativa traz, nos moldes da legislação consumerista, o princípio da qualidade dos dados (art. 3º, parágrafo 1º); o direito de acesso, retificação e cancelamento (art. 5º, II e III); a delimitação da finalidade pela qual os dados podem ser coletados e processados (art. 2º, I; art. 5º, VII e art. 7º), vedando-se a utilização dos dados para *marketing direto*, por exemplo, e, por fim, a proibição do armazenamento de informações excessivas e sensíveis (art. 3º, parágrafo 3º) (BRASIL, 2011).

Nesse contexto, tais limitações ocasionam uma limitação da coleta e das finalidades para o tratamento de dados pessoais referentes ao consumidor e, mais uma vez, buscam o capacitar para controlar as suas informações pessoais, utilizando-se o legislador, novamente, da ideia de autodeterminação informacional (BIONI, 2019).

3.2.2.4 Lei de Acesso à Informação Pública

O direito à informação é essencial para um Estado democrático e para uma administração pública transparente. Devido a isso, foi promulgada a Lei de Acesso à Informação Pública (Lei n. 12.527/2011), que entrou em vigor em maio de 2012, com o objetivo de propiciar mais transparência às atividades realizadas pelo governo,

bem como ampliar o controle dos cidadãos e concretizar o direito fundamental à informação, previsto no artigo 5º, inciso XXXIII[11]. Nesta senda, como bem nos assegura Laura Mendes, a respeito da relação entre o direito de acesso à informação pública e a proteção de dados pessoais,

> (...) **o direito de acesso à informação pública fortalece o próprio conceito de proteção de dados pessoais, ao reforçar o entendimento de que o cidadão tem direito de acessar os seus dados pessoais que estão em poder da Administração Pública (acesso do *próprio* indivíduo aos seus dados pessoais). Por outro lado, o direito à proteção de dados pessoais pode ser visto como um limite ao direito de acesso à informação, pois, em regra, terceiros não podem ter acesso aos dados pessoais do titular sem o seu consentimento; apenas sob condições específicas isso é possível**. (2014, n.p., *grifo nosso*)

Assim, é de suma importância o acesso, por parte dos cidadãos, às suas informações pessoais mantidas pelo Poder Público, uma vez que dizem respeito a sua própria personalidade. Frise-se que a lei de acesso à informação também tratou acerca do conceito de informação pessoal[12], assim como do tratamento de dados pessoais, que deve ser realizado de forma transparente, respeitando-se à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais (art. 31). Isso porque, o tratamento inadequado de dados não só é capaz de afetar o direito à privacidade, mas também diversos outros direitos fundamentais.

3.2.2.5 Marco Civil da Internet

Pode-se dizer que um Marco Civil para a *internet* compreende um conjunto de normas com a finalidade de consolidar direitos fundamentais dos cidadãos, levando-se em consideração a atual Sociedade da Informação e suas inúmeras tecnologias; delimitar a responsabilidade civil dos diversos atores inseridos nesse contexto tecnológico de comunicação e estabelecer diretrizes para a boa atuação do Estado, tanto na construção de políticas públicas quanto na criação de regulamentações específicas posteriores (CRISTINA, 2014). Convém ressaltar que a expressão "Marco Civil da Internet" é utilizada desde a tramitação do Projeto de Lei n.

[11] Art. 5º, inciso XXXIII: “todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado” (BRASIL, 1988).

[12] Art. 4º , inciso IV: “informação pessoal: aquela relacionada à pessoa natural identificada ou identificável” (BRASIL, 2011).

2.126/2011 na Câmara dos Deputados, entretanto, não foi adotada na Lei n.12.965/2014 (CRISTINA, 2014). Dessa forma, destrinchando a expressão, temos o "marco" representando o ponto de referência, o "civil" compreendendo a relação direta com os cidadãos e a "*internet*" significando a rede mundial de computadores. Tal expressão, portanto, significa nada mais do que a delimitação dos direitos do indivíduo quanto ao uso da rede mundial de computadores no âmbito brasileiro, sendo tal legislação denominada por muitos como a "Constituição da Internet" (TEIXEIRA, 2016).

Dentre as justificativas do anteprojeto de lei do Marco Civil, tinha-se que, para o Poder Judiciário, a ausência de uma referência legal específica produzia decisões judiciais conflitantes e divergentes acerca do mesmo tema, podendo colocar diversas garantias constitucionais em risco (TEIXEIRA, 2016). O MCI inaugurou, assim, uma "normativa específica para os direitos e garantias do cidadão nas relações travadas na Internet" (BIONI, 2019, p. 130) bem como supriu a lacuna normativa antes existente em relação à matéria, que era comumente julgada com base no Código Civil e no Código de Defesa do Consumidor.

Por conseguinte, uma das principais funções do MCI foi gerar segurança jurídica, de modo a oferecer uma base legal ao Poder Judiciário quando do enfrentamento de questões envolvendo *internet* e tecnologia da informação (JESUS, MILAGRE, 2014). Frise-se que foi a primeira lei criada de forma colaborativa entre governo e sociedade, tendo sido realizadas duas fases de consulta pública pelo Ministério da Justiça, a primeira iniciada no ano de 2009. A *internet* foi, então, utilizada como plataforma de debate e foi dada aos cidadãos a oportunidade de se expressarem "sobre temas como o direito ao acesso, liberdade de expressão e privacidade, não discriminação de conteúdos", resolução de conflitos ligados diretamente à rede, dentre outros (CRISTINA, 2014, p. 109).

Nesse contexto, é importante analisar alguns dos dispositivos trazidos pela mencionada lei, não sendo objeto deste trabalho esgotar o seu conteúdo, mas sim elencar as principais características advindas com a sua promulgação. Os fundamentos que disciplinam o uso da internet no território brasileiro são enumerados no art. 2º do MCI, podendo-se citar, como exemplo, a liberdade de expressão, os direitos humanos, o reconhecimento da escala mundial da rede, a pluralidade, a diversidade, a livre iniciativa e a livre concorrência. No "*caput*" do

artigo, o legislador fez questão de destacar o direito a "liberdade de expressão", não sendo permitida a censura ou remoção de conteúdos que promovam mero "dissabor" por parte dos usuários que não concordam com determinados assuntos. Dessa forma, a liberdade de expressão prevalecerá, conquanto que não viole direitos de terceiros (JESUS, MILAGRE, 2014).

O art. 3º do MCI nos apresenta diversos princípios que devem ser observados quando do uso da *internet* no Brasil. Assim, nesse contexto, o diploma normativo mais uma vez revela a importância da liberdade de expressão, elencando-a, agora, como um princípio, fazendo alusão a própria Constituição Federal. Ademais, a privacidade e a proteção de dados tornam-se princípios, pondo a salvo informações textuais ou audiovisuais que sejam consideradas privadas, bem como aquelas que sejam capazes de identificar uma pessoa, comumente requeridas por provedores de *internet* e de serviços (JESUS, MILAGRE, 2014). O parágrafo único do referido artigo destaca a não taxatividade do rol de princípios trazidos pelo MCI, não se excluindo outros previstos no ordenamento pátrio e em tratados internacionais que o Brasil seja parte.

Na sequência, o art. 4º do dispositivo legal elenca os principais objetivos do uso da *internet*, destacando-se a ideia de acesso por todos (inciso I). A preocupação com a inclusão digital e a busca pela redução das desigualdades no acesso às tecnologias da informação se faz presente em todo texto do MCI, devendo o Estado promover e fomentar estudos referentes ao uso e desenvolvimento da *internet* no país (art. 27 e 28), de forma a capacitar os estudantes, em todos os níveis de ensino, a utilizá-la de forma responsável e consciente (art. 26). Deve ser vista, portanto, como uma grandiosa ferramenta para o exercício da cidadania, promoção da cultura e desenvolvimento tecnológico, sendo responsabilidade dos entes públicos atuar de forma transparente, democrática, não-discriminatória e colaborativa.

Dentre os direitos elencados no artigo 7º, convém destacar, novamente, a privacidade e a proteção de dados pessoais, tidos como pilares do MCI, ao lado da liberdade de expressão. Com efeito, o titular dos dados foi eleito como protagonista no que concerne a proteção das suas informações pessoais, verificando-se a necessidade do seu consentimento para a coleta, o uso, o armazenamento, o tratamento e a transferência de seus dados a terceiros (art. 7º, VII e IX e art. 16). O

consentimento deve ser livre, expresso e informado (art. 7º VI, VIII, IX e XI), existindo a necessidade de prestação de informações claras e completas por aqueles que realizam tratamento de dados, mediante a utilização de cláusulas contratuais destacadas e políticas de uso públicas (BIONI, 2019). O usuário poderá, ainda, requerer a exclusão definitiva de seus dados pessoais quando fornecidos a uma determinada aplicação, desde que encerrada a relação entre as partes (art. 7º, X).

3.2.2.6 Lei Geral de Proteção de Dados (LGPD)

Após longos anos de debate, o Brasil aprovou uma Lei Geral de Proteção de Dados Pessoais. A discussão iniciou-se em 2010 e gerou diversos debates e consultas públicas até o momento da sua aprovação final, que representou grande avanço a respeito do tema[13]. Assim, até a edição da LGPD em 2018, o Brasil não possuía uma norma geral sobre proteção de dados, sendo o assunto tratado de forma extremamente dividida por meio de diversas leis setoriais, as mais relevantes delas, para a doutrina, já analisadas acima. Tal fato gerava inúmeras críticas, tanto pela insegurança jurídica à qual inúmeras empresas estavam submetidas, vez que apresentavam como pilar do negócio o tratamento de dados pessoais, quanto pela fragilidade de proteção do titular de dados (MENDES, 2019).

Dessa forma, vozes de defesa para edição de uma lei geral comumente ecoavam na doutrina brasileira, e apregoavam a necessidade de um sistema coerente de regras e parâmetros para o tratamento de dados no país. Diversos fatores externos contribuíram no processo de aprovação da legislação, como, por exemplo, o advento do Regulamento Europeu sobre proteção de dados (GDPR), em 2018; o episódio envolvendo a empresa Cambridge Analytica e a utilização maciça de dados do *Facebook*, de modo a influenciar tanto o resultado das eleições norte-americanas em 2016 (MENDES, 2019, p. 2), quanto a saída do Reino Unido da

[13] A linha do tempo em torno da discussão pode ser analisada no seguinte artigo: BIONI, Bruno. *De 2010 a 2018: a discussão brasileira sobre uma lei geral de proteção de dados pessoais.* Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em 21 nov. 2019.

União Europeia, popularmente conhecido como *Brexit*[14]; o escândalo de espionagem realizado pelo governo americano e revelado pelo ex-analista Edward Snowden, da Agência Nacional de Segurança dos Estados Unidos, fato que igualmente repercutiu na aprovação do Marco Civil da Internet (BIONI, 2019).

A utilização de dados para manipulação da sociedade, até mesmo da democracia, desencadeou a discussão sobre a necessidade, cada vez mais urgente, de se regular o seu uso. O Brasil seguiu, portanto, a tendência mundial de adoção de lei geral pra proteção de dados pessoais dos indivíduos, "consolidando e complementando o marco normativo da sociedade da informação" (MENDES, 2019, p. 2).

A LGPD (Lei n. 13.709 /2018) se preocupa, nesse contexto, com a proteção de informações relacionadas à pessoa natural identificada ou identificável, sendo aplicada no tratamento de dados realizado tanto em meio *online* quanto *offline* (manual), por pessoa natural ou jurídica, de direito público ou privado[15]. O objetivo é a proteção dos direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural (art. 1º), "mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais" (VAINZOF, 2019, p. 23). Frise-se que apenas as pessoas naturais estão abarcadas pelo referido diploma normativo, não sendo os dados das pessoas jurídicas objeto de sua proteção.

Ademais, uma das principais características da novel lei reside no fato de que o tratamento de dados só poderá ser realizado dentro de algumas situações específicas, denominadas de base legal ou hipótese normativa, tratando-se de verdadeiras autorizações que obrigatoriamente deverão ser observadas. O artigo 7º da LGPD elenca dez hipóteses que possibilitam o tratamento de dados pessoais, como, por exemplo, o consentimento do titular - devendo esse ser livre, informado,

[14] Acerca do assunto: BBC NEWS. O que é o Brexit? Entenda a polêmica saída do Reino Unido da União Europeia com esta e outras 10 questões. Disponível em: <https://www.bbc.com/portuguese/internacional-46335938>. Acesso em: 21 nov. 2019. Sugere-se, ainda, o documentário *Privacidade Hackeada*, produzido pela plataforma de streaming NETFLIX: PRIVACIDADE Hackeada. Direção: Jehane Noujaim; Karim Amer. Estados Unidos da América: NETFLIX, 2019. Disponível em: www.netflix.com.br. Acesso em: 5 nov. 2019

[15] Verifica-se que a definição ora trazida pela LGPD muito se assemelha com aquela proposta pelo Regulamento Europeu (GDPR), que em seu artigo 4º (1) prevê que dado pessoal é a informação relativa a uma pessoa singular identificada ou identificável (titular dos dados). Ainda, por identificável entende-se a pessoa singular que possa ser identificada direta ou indiretamente, em especial por referência a um identificador, a exemplo do nome, número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos da identidade física, genética, mental, econômica, cultural ou social dessa pessoa singular.

inequívoco e com finalidade determinada -; o cumprimento de obrigação legal pelo controlador; a execução de um contrato do qual o titular seja parte; o tratamento realizado pela administração pública, visando à execução de políticas públicas; a proteção da vida ou incolumidade física do titular ou de terceiro; a satisfação de interesses legítimos do controlador, devendo existir sempre uma ponderação entre esses interesses e os direitos do titular de dados, dentre outros. Portanto, à semelhança do GDPR, a LGPD traz hipóteses bem definidas em que o tratamento de dados será autorizado, invertendo-se a lógica anterior de coletar os dados para, só depois, buscar uma finalidade para o seu uso.

Para além disso, a lei prevê direitos inerentes aos titulares dos dados, que são conhecidos em legislações nacionais e tratados internacionais pela sigla "ARCO": acesso, retificação, cancelamento e oposição[16] (MENDES, 2019, p. 4). Tais direitos, previstos em diversas normas analisadas, são básicos quando nos referimos a proteção de dados, posto que representam o empoderamento do titular sobre suas próprias informações pessoais e, sobretudo, na sua autonomia da vontade (BIONI, 2019).

Cumpre salientar que diversas obrigações são estabelecidas aos agentes de tratamento, quais sejam, o controlador, o operador e o encarregado[17]. A eles cabe, por exemplo, manter o registro das operações de tratamento de dados pessoais que realizarem, principalmente quando baseadas no legítimo interesse (art. 37) bem

[16] Os direitos dos titulares elencados na LGPD são: "Art. 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018).

[17] A LGPD adota os mesmos conceitos previstos no GDPR. Dessa forma, o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador e, por fim, o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL, 2018). Assim, o encarregado terá como funções: "receber reclamações dos titulares, comunicar-se com a autoridade nacional e orientar os funcionários para que a organização cumpra com as normas de proteção de dados." (MENDES, 2019, p. 4).

como adotar medidas de segurança, técnicas e administrativas no intuito de proteger os dados pessoais de acessos não autorizados. Nesse contexto,

> O capítulo de segurança da informação é um pilar fundamental da LGPD e traz pelo menos três inovações importantes para o ordenamento jurídico brasileiro quanto às obrigações dos agentes de tratamento. Em primeiro lugar, a lei exige que eles adotem medidas que garantam a integridade, a confidencialidade e a disponibilidade dos dados sob tratamento. Em segundo lugar, em caso de incidente de segurança, como o vazamento de dados, o controlador é obrigado a comunicar a autoridade de proteção de dados, que pode determinar a adoção de medidas de mitigação ou a ampla divulgação para a sociedade. Em terceiro lugar, há uma obrigação que se enquadra no conceito de *Privacy by Design*, já que tais medidas deverão ser observadas desde a fase de concepção até a execução do produto ou serviço. (MENDES, 2019, p. 4-5).

No que concerne à responsabilidade dos agentes em caso de dano decorrentes dos tratamentos de dados, a LGPD prevê que essa pode se dar tanto na forma civil quanto na forma administrativa. A responsabilidade civil dos agentes leva em consideração a natureza da atividade desenvolvida e caberá ao controlador na maioria das hipóteses estabelecidas pela lei. O operador, por sua vez, responderá pelos atos que sejam contrários à lei ou às instruções dadas pelo controlador, aplicando-se, nesse último caso, a responsabilidade solidária entre controlador e operador (art. 42). (BRASIL, 2018).

Quanto à responsabilidade administrativa, a LGPD estabelece diversas sanções que devem ser aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD). As sanções podem constituir-se em advertências, multas – no valor de até 2% do faturamento da empresa -, proibição, total ou parcial, do exercício das atividades relacionadas ao tratamento de dados (MENDES, 2019), publicização da infração após apurada a sua ocorrência – o que pode gerar danos à imagem das instituições que não seguirem as novas regras (WILLEMIN, 2019)[18], bem como a eliminação dos dados pessoais a que se refere a infração (art. 52).

Pode-se concluir, nesse contexto, que a nova Lei Geral de Proteção de Dados representou grande avanço “rumo à construção de um sistema de proteção de dados pessoais no Brasil, passo fundamental para o fortalecimento da confiança do cidadão nos serviços presentes na sociedade da informação” assim como para o

[18] Disponível em: https://www.conjur.com.br/2019-jan-28/opiniao-importancia-avanco-leis-protecao-dados. Acesso em: 20 nov. 2019.

incentivo “à inovação constante desses serviços” (MENDES, 2019, p. 6). Sabe-se que a utilização de dados por entes públicos e privados propicia excelentes serviços à sociedade, inteiramente baseados em economia de dados. Os benefícios são inúmeros, entretanto, os danos gerados por um vazamento de dados, por exemplo, pode ser irreversível, devendo existir leis contundentes aptas a proteger os direitos fundamentais dos indivíduos.

Dessa forma, apesar do progresso trazido pela LGPD, entende-se que se faz necessária a proteção constitucional dos dados pessoais no ordenamento jurídico brasileiro, uma vez que tal legislação não será “apta a proteger o cidadão de outras leis que venham a ser aprovadas pelo Poder Legislativo” (MENDES, 2019, p. 6) e que permitam o processamento abusivo de dados e a legitimação de práticas de vigilância, por exemplo. Analisar-se-ão, portanto, os principais direitos fundamentais envolvidos e a necessidade de constitucionalização do direito à proteção de dados pessoais, devendo esse direito ser vislumbrado diante de uma perspectiva autônoma.

4 DA PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL

Buscou-se, até então, demonstrar como a proteção de dados vem sendo disciplinada pelos mais variados diplomas normativos, internacionais e nacionais, tendo sido constatado que o direito à proteção de dados surgiu, inicialmente, como uma vertente do direito fundamental à privacidade. O que se pretende com a presente pesquisa, entretanto, é demonstrar que, atualmente, é necessário se falar acerca de um direito fundamental à proteção de dados pessoais como direito autônomo, por entender-se que, apenas o direito à privacidade não será suficiente para proteger os indivíduos na atual sociedade da informação.

4.1 OS DIREITOS FUNDAMENTAIS ENVOLVIDOS NO PROCESSAMENTO DE DADOS

O sistema de direitos fundamentais como um todo é influenciado pelo processamento massivo de informações, já que as tecnologias da informação atuam diretamente na concretização de diversos direitos, como a liberdade de expressão, comunicação, bem como na transformação do mundo do trabalho, da administração e do mercado. (HOFFMANN-RIEM apud MENDES, 2014).

Dessa forma, Laura Mendes (2014), magistralmente, nos traz alguns exemplos de violação a direitos fundamentais causado pelo intenso fluxo de dados pessoais. Assim, o direito à igualdade pode ser facilmente violado quando da utilização de dados pessoais para a criação de bancos de dados raciais ou de imigrantes (*racial profiling*[19]), tomando-se, a partir deles, decisões discriminatórias; a

[19]A expressão tem sido comumente usada para explicar ações policiais baseadas na raça, etnia, cor da pele e nacionalidade de um indivíduo, em vez de sustentar-se, exclusivamente em seu comportamento. Justifica-se, assim, a ação policial contra determinados grupos, afirmando que eles estão propícios a cometer delitos mais do que outros. Como recente exemplo, têm-se as abordagens policiais realizadas em ônibus públicos provenientes de comunidades em direção às praias da zona Sul da cidade do Rio de Janeiro. A ação dos policiais "compreendia em apreender jovens provenientes de bairros como Jacarezinho, Manguinhos, entre outras comunidades pobres da cidade ou da Baixada Fluminense como forma de prevenção. A polícia classificou que jovens pretos e pardos, sem documentos, sem dinheiro, vindos de favelas e com menos de 18 anos deveriam se enquadrar na condição de criminoso em potencial e, assim, serem custodiados pelo Estado". (COSTA C., FERES JÚNIOR, 2015). Disponível em: https://www.cartamaior.com.br/?/Editoria/Direitos-Humanos/Racial-profiling-e-direitos-do-cidadao-as-contradicoes-de-uma-politica-de-seguranca-publica-racista/5/34623. Acesso em: 25 nov. 2019. Outros exemplos de racial profiling podem ser encontrados no *site* da União Americana pelas Liberdades Civis, ONG norte-americana sediada na cidade de Nova Iorque. Disponível em: https://www.aclu.org/other/racial-profiling-definition. Acesso em 25 nov. 2019.

recusa na contratação de um empregado devido ao fato de seu nome constar em bancos de dados referentes a indivíduos que já ajuizaram ações trabalhistas pode afetar a liberdade de exercício de trabalho[20]; o acesso a dados genéticos como influenciador na contratação igualmente pode violar o livre exercício do trabalho, bem como o direito de ir e vir pode ser facilmente limitado com a proibição de embarque em aeronaves de passageiros que possuem seus nomes equivocadamente inseridos em listas de terroristas, conhecidas como "*No Fly List*".

Tais direitos, violados quando do processamento massivo de dados, não são abarcados pelos principais dispositivos que regulamentam as consequências da utilização massiva da informação, quais sejam, os incisos X e XII do art. 5º da Constituição Federal (BRASIL, 1988):

> Art. 5º (...)
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> (...)
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Acerca dos exemplos ora trazidos, tem-se que as informações pessoais que dizem respeito à origem racial e étnica, aptas a constituir bancos de dados voltados ao *racial profiling*, apesar de sensíveis, provavelmente não seriam consideradas como íntimas ou referentes à vida privada, assim como não se enquadrariam no conceito de correspondência ou comunicação de dados, muito menos poderiam ser entendidas como sigilosas (MENDES, 2014). Parece-nos, como já mencionado, que o principal direito fundamental violado é o da igualdade, uma vez que os Estados se utilizam de dados pessoais sensíveis para efetivar políticas de segurança discriminatórias e segregacionistas, demonstrando que a questão está longe de ser contemplada apenas pelos incisos X e XII do art. 5º da CRFB/88.

Ademais, as informações concernentes ao ajuizamento de ações trabalhistas, aptas a formar bancos de dados capazes de discriminar os

[20] O TST vem reconhecendo a ilegalidade de listas discriminatórias, vez que essas violam direitos decorrentes da própria dignidade humana. Nesse sentido: Processo nº TST-RR-579-43.2010.5.09.0091, julgado em 24 de mai. de 2017, rel. Min. Cláudio Brandão, 7ª Turma. Disponível em: https://www.migalhas.com.br/arquivos/2017/8/arq20170803-05.pdf. Acesso em: 25 nov. 2019. Acerca do assunto: https://examedaoab.jusbrasil.com.br/noticias/485830808/empresa-de-rh-e-condenada-por-manter-lista-suja-com-nomes-de-funcionarios-que-ajuizaram-acao. Acesso em: 25 nov. 2019.

trabalhadores que recorrem ao Poder Judiciário para pleitear direitos, tampouco poderiam ser consideradas íntimas ou privadas. O ordenamento jurídico brasileiro as considera como públicas de uma maneira geral, excetuadas as situações de sigilo (MENDES, 2014).

Por conseguinte, a exigência de testes genéticos para os empregados, como requisito para contratação ou promoção, se enquadra tanto no âmbito de proteção da intimidade e privacidade quanto no campo do direito ao trabalho[21], da não discriminação[22] e do direito à igualdade. Pode-se falar, até mesmo, em um direito à identidade genética[23], associado às ideias de proteção do indivíduo contra ingerências no seu genoma e à autodeterminação pessoal (VIANA R., 2013).

Ainda com base em tal exemplo, a evolução da pesquisa genética e do desenvolvimento do Projeto Genoma Humano[24] (PGH), apesar dos diversos avanços que ofereceram à humanidade, trouxera consigo incertezas éticas, legais e sociais (PENA e AZEVÊDO, 1998). Assim, por detrás do conhecimento de dados genéticos, existem disputas, interesses financeiros e econômicos de laboratórios, companhias de seguro de vida e seguro-saúde, assim como de empregadores (ZATZ, 2000), uma vez que os dados genéticos dos indivíduos indicam, cada vez mais, as suas competências e possíveis patologias futuras. Utiliza-se a informação

[21] Art. 5º, XIII: "é livre o exercício de qualquer trabalho, ofício ou profissão, atendidas as qualificações profissionais que a lei estabelecer" (BRASIL, 1988). Cumpre ressaltar que tal direito possui duas dimensões prestacionais, sendo elas: a positiva, atrelada diretamente ao dever do Estado, bem como entidades patronais, de executar políticas de fomento ao emprego e acesso a oportunidades igualitárias; e a negativa, que refere-se justamente à proteção contra possíveis discriminações existentes quando do acesso a cargos e profissões (VIANA R., 2013).

[22] Art. 7º, XXXI: "proibição de qualquer discriminação no tocante a salário e critérios de admissão do trabalhador portador de deficiência" e Art. 7º, XXXII: "proibição de distinção entre trabalho manual, técnico e intelectual ou entre os profissionais respectivos" (BRASIL 1988).

[23] O art. 26, 3, da Constituição de Portugal, que determina "Outros direitos pessoais", prevê que "a lei garantirá a dignidade pessoal e a identidade genética do ser humano, nomeadamente na criação, desenvolvimento e utilização das tecnologias e na experimentação científica". (PORTUGAL, 1976). Disponível: https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx. Acesso em: 25 nov. 2019.

[24] O Projeto Genoma Humano (PGH) beneficiou a evolução da medicina curativa, preventiva e preditiva, essa última voltada à realização de predições quanto às possibilidades e riscos de desenvolvimento de doenças futuras (FARIAS, CANDIDO, 2010). Dessa forma, mediante o estudo da biogenética, buscou-se identificar os genes humanos, determinar a sequência dos cerca de 3,2 bilhões de pares de bases que compõem o genoma do *Homo Sapiens*, armazenar tais informações em bancos de dados, assim como desenvolver ferramentas para o processamento dos dados. O conhecimento gerado por tal pesquisa gerou profundo impacto na maneira como as doenças são diagnosticadas, tratadas e prevenidas, mudando drasticamente a prática clínica e na saúde pública. As sequências do genoma humano estabelecem uma rica fonte de informação biológica que ajudará a pesquisa e descoberta de milhares de aplicações práticas, criando-se um verdadeiro tesouro de dados que fornecerão maior clareza e conhecimento do processo molecular que define a vida. Disponível em: http://genoma.ib.usp.br/sites/default/files/projeto-genoma-humano.pdf. Acesso em 25 nov. 2019.

genética pessoal como forma de impossibilitar o acesso ou permanência na atividade laborativa, fato esse apto a gerar grande discriminação no seio da sociedade.[25]

Ademais, tem-se que a investigação de dados referentes a suspeita de prática de crime é interesse social a ser ponderado com os direitos individuais. O seu processamento e conhecimento são indispensáveis à sociedade. Entretanto, quando inseridos indevidamente em listas e bancos de dados governamentais, podem gerar danos aos direitos fundamentais e ao próprio princípio da presunção da inocência. Tal prática, extremamente comum nos Estados Unidos, no tocante ao combate ao terrorismo, igualmente pode violar o direito ao devido processo, conforme a decisão do juiz federal Anthony Trenga do Estado da Virgínia, em relação ao direito de ir e vir em aeroportos. A decisão, datada de 4 de setembro de 2019, afirma que:

> O governo não notifica as pessoas incluídas na lista, não dá explicações sobre os critérios ou provas usadas para determinar o status de suspeitas de terrorismo e não oferece qualquer processo para retirar o nome delas da lista. (TRENGA, 2019 apud MELO, 2019a)[26]

Nesse contexto, o magistrado considerou que a lista de observação mantida pelo FBI e pelo Departamento de Segurança Nacional dos Estados Unidos, pode violar diversos direitos constitucionais dos cidadãos. Assim, trata-se de um verdadeiro banco de dados criado mediante o monitoramento constante dos indivíduos, no qual diversas pessoas inocentes podem ser registradas por meio de denúncias falsas, transações financeiras, histórico de viagens, negócios que desenvolve, ou, até mesmo, por aprender árabe (MELO, 2019a) [27]. Destaque-se que, a autodeterminação informacional, eleita em numerosos diplomas normativos (item 3.2 *supra*) como referência quando do tratamento de dados, é desconsiderada em tais situações, visto que os indivíduos não possuem controle acerca da coleta, processamento e compartilhamento das suas informações pessoais.[28]

---

[25] Acerca do assunto: ARAUJO, Antonio Castro Alves. *Discriminação genética é uma ameaça ao trabalhador.* Disponível em: https://www.conjur.com.br/2010-jul-28/discriminacao-genetica-ameaca-integridade-moral-trabalhador. Acesso em: 25 nov. 2019.

[26] Decisão original disponível em: https://int.nyt.com/data/documenthelper/1689-terror-watchlist-ruling/75cd50557652ad0bfa2a/optimized/full.pdf#page=1. Acesso em: 26 nov. 2019.

[27] Disponível em: https://www.conjur.com.br/2019-set-10/eua-lista-suspeitos-terrorismo-viola-direitos-constitucionais#top. Acesso em: 20 nov. 2019.

[28] Os cidadãos encontram diversos obstáculos para retirar informações pessoais de tais listas, já que o governo norte-americano dificulta sobremaneira tal processo. Em documentos liberados pelo próprio FBI ao The New York Times, em virtude de uma ação judicial, constatou-se que, ainda que o

Nesse cenário, é comum a todos os casos ora analisados a utilização de dados que individualizam e qualificam uma determinada pessoa, sem que se configurem necessariamente em dados íntimos ou privados (MENDES, 2014). Isso porque, o direito à privacidade tem por objeto “os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público.” (MENDES, BRANCO, 2015, p. 280). Já o “objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas” (MENDES, BRANCO, 2015, p. 280), por exemplo.

Marcelo Novelino ao tratar acerca do tema, afirma que,

> A **intimidade** está relacionada ao modo de ser de cada pessoa, ao mundo intrapsíquico aliado aos sentimentos identitários próprios (autoestima, autoconfiança) e à sexualidade. Compreende os segredos e as informações confidenciais. A **vida privada** abrange as relações do indivíduo com o meio social nas quais não há interesse público na divulgação. (2016, p. 337, *grifo do autor*).

Pode-se dizer que a privacidade, portanto, “compreende todos os domínios da vida da pessoa que lhe são próprios e que lhe dizem respeito” ao passo que a intimidade corresponde ao “núcleo do direito à privacidade”, constituindo a parte mais íntima dessa (VIANA R., 2013, p. 81), tratando-se de verdadeira esfera secreta da vida do indivíduo (DOTTI, 1980, p. 69).

Assim, verifica-se que o direito à privacidade, intimidade e garantia ao sigilo protegem o indivíduo em face de diversos riscos, como a divulgação de informações íntimas ou interceptação das comunicações. Entretanto, não abarcam os riscos aos quais os indivíduos estão sujeitos na sociedade contemporânea, percebendo-se que os dados pessoais merecem proteção a nível constitucional, vez que, como visto, o seu processamento e utilização geram violação a direitos fundamentais diversos.

É necessário ressaltar que a interpretação usual no ordenamento jurídico brasileiro acerca da expressão “sigilo de dados”, presente no inciso XII do art. 5º da CRFB/88, compreende apenas a comunicação de dados (MENDES, 2014). Tal

---

indivíduo seja inocentado por um tribunal dos Estados Unidos, o seu nome poderá permanecer em bancos de dados se os agentes acreditarem que ainda existe uma “suspeita razoável” (MELO, 2011b). Disponível em: https://www.conjur.com.br/2011-set-29/fbi-considera-todos-culpados-lista-mesmo-prove-contrario. Acesso em: 20 nov. 2019.

entendimento foi adotado em diversos julgados do Supremo Tribunal Federal[29] e é bem explicitado por Tercio Sampaio Ferraz Jr:

> O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "'da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Note-se, para a caracterização dos blocos, que a conjunção "*e"* une correspondência com telegrafia, segue-se um a vírgula e depois, a conjunção de dados com comunicações telefônicas. Há um a simetria nos dois blocos. Obviamente o que se regula é *comunicação* por correspondência e telegrafia, *comunicação* de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não estará havendo quebra de sigilo. Mas se alguém *entra nesta transmissão*, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. **A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) *privativa* é que não pode ser violada por sujeito estranho à comunicação.** (1993, p. 446-447, *grifo nosso*)

Existem entendimentos, ainda, no sentido de que a proteção de dados prevista no artigo 5º, inciso XII, garante a privacidade do indivíduo em relação a informações fiscais e bancárias dos indivíduos, independentemente de se encontrarem armazenadas em bancos de dados de instituições financeiras, da Receita Federal ou de outro órgão do poder público (MORAES, 2018). Assim, a presente pesquisa compartilha do entendimento de o "sigilo de dados", previsto no supracitado artigo, não se refere à proteção de dados pessoais em si, merecendo destaque as colocações do autor Danilo Doneda,

> **A leitura das garantias constitucionais para os dados somente sob o prisma de sua comunicação e de sua eventual interceptação lastreia-se em uma interpretação que não chega a abranger a complexidade do fenômeno da informação ao qual fizemos referência.** Há um hiato que segrega a tutela da privacidade, esta constitucionalmente protegida, da tutela das informações pessoais em si [...]. E este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar novamente o quanto hoje em dia as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas

[29] RExt 418.416, Santa Catarina, rel. Min. Sepúlveda Pertence, 10-5-2006; HC 91.867, Pará, rel. Min. Gilmar Mendes, 24-4-2012.

> mediante a representação de sua personalidade, fornecida pelos seus dados pessoais, aprofundando ainda mais a íntima relação entre tais dados e a própria identidade e personalidade de cada um de nós. **Apenas sob o paradigma da interceptação, da escuta, do grampo – situações que são apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias – não é possível proporcionar uma tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece.** (2011, p.106, *grifo nosso*)

Superada tal questão, verifica-se que é de extrema necessidade que o ordenamento jurídico se reconstrua e reinvente, de modo a assimilar e solucionar os novos problemas enfrentados na sociedade da informação. Para tanto, a Constituição deve adaptar-se às transformações históricas e sociais, de modo a tutelar os indivíduos contra as formas de abuso de poder que emergem na sociedade, sob pena de se tornar uma mera folha de papel, como bem lecionado por Ferdinand Lassalle (2000).

Nesse contexto, a Constituição deve demonstrar, de um lado, permanência, continuidade, estabilidade e segurança e, de outro, flexibilidade e abertura para novas interpretações e atualizações, de forma a concretizar princípios e direitos nela inseridos. Trata-se de uma verdadeira compreensão dinâmica do texto constitucional, sujeito a alterações interpretativas mediante um processo aberto e plural, no qual toda a sociedade tem o direito de participar (HÄBERLE apud MENDES, 2014). Portanto, analisando e reinterpretando o conceito de privacidade, temos que tal direito fundamental evoluiu nas últimas décadas, fazendo surgir um novo direito inerente a todos os indivíduos: o direito à proteção de dados pessoais.

Assim, a partir de uma interpretação sistemática da Constituição Federal, que prevê o princípio da dignidade da pessoa humana, a ação constitucional do *habeas data*, a qual reconhece a importância da informação pessoal por possibilitar o conhecimento e retificação de dados relativos à pessoa do impetrante em bancos de dados de caráter público, bem como o direito à privacidade e intimidade, temos que é possível extrair da mesma um direito fundamental à proteção de dados. O reconhecimento desse direito, por parte do legislador e de toda a sociedade, é de extrema importância para efetivar os fundamentos e princípios de um Estado Democrático de Direito (MENDES, 2014).

Frise-se que, com o reconhecimento de um direito material à proteção de dados, a utilização limitada do *habeas data* poderia ser ampliada e haveria novas possibilidades para o ajuizamento de tal ação (MENDES, 2014). A sua aplicação

poderia ser ampliada não só ao acesso e retificação dos dados, mas também à possibilidade do seu cancelamento. É o que se depreende do entendimento esposado por Gilmar Mendes ao afirmar que:

> É interessante notar que, diferentemente do que se poderia esperar, o *habeas data*, na forma expressa na Constituição, ficou limitado, em princípio, ao conhecimento e à retificação de dados existentes em bancos de dados governamentais ou de caráter público. Tal abordagem mostra um déficit de concepção no aludido instrumento processual, ao revelar que talvez o objeto de proteção tenha acabado por ficar demasiadamente restrito (conhecimento ou retificação de dados). (MENDES, BRANCO, 2015, p. 451).

Ademais, uma breve análise comparativa com o direito estrangeiro é capaz de demonstrar o reconhecimento à proteção de dados/informações pessoais a partir de diferentes formas, em variados ordenamentos jurídicos. Na Alemanha, como visto, na decisão da Corte Constitucional Alemã no julgamento da Lei do Censo, foi reconhecido o direito à autodeterminação informativa (MENDES, 2014); em Portugal, a Constituição prevê, em seu art. 35[30], a "Utilização da Informática", regulamentando as condições de utilização e processamento dos dados pessoais (PORTUGAL, 1976) e na Espanha, a Constituição (ESPANHA, 1978) regulamenta, de forma semelhante, que a lei limitará o uso da informática, de modo a garantir a honra e a intimidade pessoal e familiar dos cidadãos.

Ainda, a Carta de Direitos Fundamentais da União Europeia[31] pressupõe, de maneira precisa, a proteção de dados como um direito fundamental, a necessidade de consentimento do titular ou outro fundamento legal para o tratamento, assim

---

[30] "Artigo 35.º Utilização da informática.
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 manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei." (PORTUGAL, 1976).

[31] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR. Acesso em: 28 nov. 2019.

como a necessidade de criação de autoridades administrativas para o controle de tal atividade (MENDES, 2014). No Chile, a Lei nº 21.096 de 2018 foi responsável por alterar a Constituição do país de 1980, de forma a consagrar o direito à proteção dos dados pessoais em seu artigo 19, número 4 (CHILE, 1980)[32].

4.2 DA PERSPECTIVA DE UM DIREITO FUNDAMENTAL AUTÔNOMO

O direito à proteção de dados possui objeto multidimensional, que não envolve apenas direitos de primeira dimensão, como o tradicional direito à privacidade, mas também aspectos de outras esferas protetivas, como, por exemplo, os direitos consumeristas e direitos políticos. Em relação às novas dimensões (ou gerações) dos direitos fundamentais, não existe um consenso entre os doutrinadores, vez que cada um deles costuma realizar a sua própria classificação. Para os autores José Alcebíades Júnior e Antonio Wolkmer, por exemplo, "os direitos vinculados aos benefícios da sociedade tecnológica e da informação, do Ciberespaço, da Internet e da realidade virtual em geral" (apud SARLET, MARINONI, MITIDIERO, 2018, p. 337) estariam inseridos na quinta dimensão dos direitos fundamentais.

Ainda nesse sentido, alguns autores da área do direito eletrônico, como Patrícia Pinheiro e Luis Carlos Olivo (apud OLIVEIRA, LAZZARI, 2017), entendem que a quinta dimensão envolvem "o direito de acesso e convivência numa ambiente salutar no ciberespaço" (OLIVEIRA, LAZZARI, 2017, p. 147), cumprindo mencionar que, há uma relativa convergência na doutrina em se afirmar que as "interações entre homem e novas tecnologias" estão situadas na quinta dimensão dos direitos fundamentais (OLIVEIRA, LAZZARI, 2017, p. 148).

4.2.1 Âmbito de proteção e titularidade

[32] Disponível em: https://www.hipervinculos.cl/se-publico-en-diario-oficial-reforma-constitucional-de-proteccion-de-datos-personales/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original. Acesso em: 28 nov. 2019. Nesse sentido: "Proyecto de reforma constitucional: "Artículo único. – Agrégase, em el numeral 4º del artículo 19 de la Constitución Política de la República, a continuación de la expresión "y su família", lo seguinte: ", y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley". Disponível em: https://www.leychile.cl/Navegar?idNorma=1119730. Acesso em: 28 nov. 2019.

Pode-se dizer que o âmbito de proteção do direito fundamental à proteção de dados envolve a utilização e processamento das informações pessoais em geral. A relevância jurídica se fundamenta justamente nos processos de coleta, armazenamento, utilização e transferência, a partir dos quais são extraídas informações a serem usadas em um determinado contexto para certa finalidade (ALBERS apud MENDES, 2014). Assim sendo, a proteção constitucional entrará em ação quando da utilização de informações pessoais em atividades que causem riscos aos interesses legítimos dos cidadãos, não amparados por outros direitos fundamentais, de forma individual ou conjunta, como aquelas cuja exposição possa ensejar condutas discriminatórias.

Nesse contexto, tal direito fundamental consiste na proteção dos cidadãos contra os riscos que ameaçam a sua personalidade quando da utilização de seus dados pessoais, por entes públicos e privados, bem como na atribuição ao indivíduo da garantia de autodeterminar seus dados na sociedade (MENDES, 2014). Merece destaque, ainda, a doutrina alemã, que entende a proteção de dados como forma de tutelar tanto a integridade moral e a personalidade dos indivíduos, quanto à proteção do direito geral à liberdade, como a liberdade de comunicação, trabalho, locomoção, informação, dentre outras (BRITZ apud MENDES, 2014).

No que tange à titularidade, primeiramente cumpre realizar uma diferenciação. Titular do direito é aquele que figura como “sujeito ativo da relação de direito subjetivo”, sendo o sujeito de direito, enquanto destinatário é a pessoa física, jurídica, ou até mesmo o ente despersonalizado, “em face do qual o titular pode exigir o respeito, a proteção ou a promoção do seu direito” (SARLET, MARINONI, MITIDIERO, 2018, p. 374). Ademais, “de acordo com o princípio da universalidade, todas as pessoas, pelo fato de serem pessoas, são titulares de direitos e deveres fundamentais” (SARLET, MARINONI, MITIDIERO, 2018, p. 375).

Assim, partindo do princípio de que os “dados pessoais” são informações relativas à pessoa natural, identificada ou identificável, e pelo fato de se ligarem fortemente à própria personalidade do indivíduo, assim como o direito fundamental da dignidade da pessoa humana, defende-se que somente as pessoas físicas são titulares de tal direito (MENDES, 2014). A doutrina alemã apresenta-se no mesmo sentido, entendendo que tanto as pessoas jurídicas de direito público quanto as de direito privado não são titulares do direito à autodeterminação informativa (direito à

proteção de dados). Afirma que, para a proteção desses entes, há outros direitos fundamentais mais adequados (MENDES, 2014), no quanto forem compatíveis com a sua natureza dessas pessoas. Segundo bem explicita Maíra Carneiro, quando da edição do Projeto de Lei de Proteção de Dados,

> Cumpre esclarecer, contudo, que o Projeto de Lei de Proteção de Dados Pessoais somente resguarda os dados de pessoas naturais. Isto porque, segundo o próprio Ministério da Justiça, 'não é necessário nem desejável estender às empresas instrumentos de proteção que foram concebidos para a proteção de um direito fundamental do cidadão', uma vez que, segundo o entendimento do órgão ministerial, para a tutela das informações da pessoa jurídica devem ser utilizadas normas que protejam os interesses patrimoniais, e não pessoais. Ademais, hoje as empresas já possuem diversos instrumentos para a proteção de seus dados, de forma que não seria pertinente contemplá-las no texto do PL no presente momento, mas sim, futuramente, cogitar a possibilidade da edição de lei específica para regularizar a proteção dos dados das pessoas jurídicas diante das novas tecnologias da informação, da mesma forma que está sendo feito com as pessoas físicas no PL. (2016, p. 146).

4.2.2 Dimensão Objetiva e Subjetiva

A dimensão subjetiva dos direitos fundamentais diz respeito à possibilidade, que possui o titular do direito, de impor judicialmente os seus interesses juridicamente tutelados em face do destinatário (SARLET, MARINONI, MITIDIERO, 2018). Assim, nessa dimensão ou perspectiva, "os direitos fundamentais correspondem à exigência de uma ação negativa (em especial, de respeito ao espaço de liberdade do indivíduo) ou positiva de outrem" (MENDES, BRANCO, 2015, p. 167). Nos dizeres de José Vieira de Andrade, é nada mais do que a:

> proteção de uma determinada esfera de autorregulamentação ou de um espaço de decisão individual; tal como é associado a um certo poder de exigir ou pretender comportamentos ou de produzir autonomamente efeitos jurídicos. (2001, p. 163)

Nesse contexto, o direito fundamental à proteção de dados pessoais, quando analisado em sua dimensão subjetiva, consiste em um direito de defesa, que concede ao cidadão um espaço de liberdade, não submetido a intervenções estatais (MENDES, 2014), bem como privadas. Em caso de violação ou ameaças, garante, respectivamente, a cessação da intervenção e a tomada de ações preventivas para a sua não ocorrência. Ademais, pressupõe que as restrições legais a tal direito fundamental não acarretem a sua eliminação, sob pena de virem a ser consideradas inconstitucionais.

Conforme bem preceitua Laura Mendes, o controle dos dados pessoais pelo indivíduo consiste em aspecto primordial da dimensão subjetiva, uma vez que os dados se referem a ele e influenciam a sua esfera de direitos (MENDES, 2014). Apenas o titular pode definir o alcance da circulação de seus dados, fato esse que, todavia, mostra-se de dificílima observância na sociedade da informação.

Os direitos fundamentais, vistos a partir de uma dimensão objetiva, representam decisões valorativas de natureza jurídico-objetiva que incidem no ordenamento jurídico como um todo. Referem-se, portanto, a um conjunto de valores básicos e fins diretivos para os Poderes Públicos, não se restringindo aos interesses individualmente considerados (SARLET, MARINONI, MITIDIERO, 2018). Pode-se citar, como exemplo de desdobramento da perspectiva objetiva, a eficácia irradiante dos direitos fundamentais, uma vez que fornecem diretrizes e impulsos para a aplicação do direito infraconstitucional.

Relacionado a esse efeito, outra característica diz respeito à necessidade de adoção, por parte do Estado, de deveres de proteção, de forma a impor aos órgãos estatais a obrigação permanente de tutelar os direitos fundamentais dos cidadãos contra violações por parte dos poderes públicos, dos particulares e, até mesmo, de outros Estados (SARLET, MARINONI, MITIDIERO, 2018). Ademais, faz-se necessária a menção às normas organizatórias e procedimentais, influenciadas diretamente por todo o sistema de direitos fundamentais, o qual também por elas é influenciado. Os deveres de proteção do Estado se concretizam, em muitos casos, com a adoção de normas que dispõem acerca de procedimentos administrativos e judiciais, assim como pela formação de órgãos responsáveis pela tutela e promoção de direitos – a fruição desses se perde em efetividade ou, até mesmo, não se faz possível, se não implementadas por prestações estatais no âmbito procedimental ou organizacional (SARLET, MARINONI, MITIDIERO, 2018).

Assim, como bem colacionado por Gilmar Mendes,

> A dimensão objetiva resulta do significado dos direitos fundamentais como princípios básicos da ordem constitucional. [...] Esse fenômeno faz com que os direitos fundamentais influam sobre todo o ordenamento jurídico, servindo de norte para a ação de todos os poderes constituídos. [...] a dimensão objetiva dos direitos fundamentais cobra a adoção de providências, quer materiais, quer jurídicas, de resguardo dos bens protegidos. Isso corrobora a assertiva de que a dimensão objetiva interfere na dimensão subjetiva dos direitos fundamentais, neste caso atribuindo-lhe reforço de efetividade. [...] A dimensão objetiva enseja, ainda, a discussão sobre a eficácia horizontal dos direitos fundamentais – a eficácia desses

> direitos na esfera privada, no âmbito das relações entre particulares. (MENDES, BRANCO, 2015, p. 167-169)

De forma semelhante, Laura Mendes (2014) dispõe que a dimensão objetiva pressupõe a necessidade de concretização de tais direitos pelo legislador, que deve estabelecer tanto os procedimentos e condições de exercício, quanto os mecanismos de proteção do bem jurídico, ambos pressupondo a ação positiva do Estado.

Assim, quanto ao direito à proteção de dados, quando verificado o aspecto procedimental, tem-se que é dever do poder público regulamentar as condições de tratamento, de modo a garantir os princípios da transparência (deve o titular conhecer o responsável pelo processamento, bem como quais dados estão sendo processados), finalidade (o tratamento deve respeitar o contexto no qual os dados foram coletados), segurança (proteção contra extravios e vazamentos de dados) e do esquecimento (limite temporal para o armazenamento de dados pessoais). Ainda, devem existir métodos para assegurar os direitos de acesso, retificação e cancelamento em face de bancos privados e públicos, objetivando o efetivo controle do titular sobre os seus dados pessoais (MENDES, 2014).

Quanto aos deveres de proteção, à proteção de dados enseja a ação dos três poderes, Legislativo, Judiciário e Executivo. O primeiro tem o dever de promover a arquitetura institucional adequada, elaborando normas eficientes para a tutela do cidadão face ao processamento desenfreado de dados. O poder Judiciário deve atuar quando ausente ou insuficiente o poder Legislativo, assegurando a proteção a partir de normas já existentes[33]. Por fim, o poder Executivo é responsável pela criação de estruturas administrativas e de controle, capaz de promover a proteção constitucional (MENDES, 2014). Destaque-se que, nesse último caso, a Lei Geral de Proteção de Dados prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD) [34], órgão da Administração Pública Federal, integrante da Presidência da

[33] Nesse sentido, a LGPD prevê, em seu artigo 22 que “A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual ou coletiva.”. Ademais, a lei prevê um benefício ao titular dos dados, qual seja a inversão do ônus da prova no processo civil, quando for verossímil a sua alegação, houver hipossuficiência para fins de produção de prova ou, ainda, quando a produção de prova resultar-lhe excessivamente onerosa (BRASIL, 2018). Trata-se de verdadeiro amparo ao titular de dados, que não possui, na maior parte das vezes, paridade de armas se comparado às grandes empresas e ao poder público.

[34] As competências da ANPD são elencadas no art. 55-J da LGPD, dentre as quais se destacam: a proteção dos dados pessoais, nos termos da legislação; elaboração de diretrizes para a Política

República (BRASIL, 2018), bem como do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, composto por representantes dos mais variados setores sociais (órgãos públicos, sociedade civil, instituições científicas, confederações sindicais, dentre outros). (BRASIL, 2018).

Ademais, a proteção aos dados pessoais enseja um dever de proteção estatal em relação ao consentimento dos indivíduos que, em geral, não é verdadeiramente livre e esclarecido, apesar das diversas normas que preveem tal condição para o tratamento. Tal consentimento, portanto, não isenta o dever geral de cuidado e proteção nem a responsabilidade dos agentes, eis que insuficiente e inadequado na prática.

A realidade é uma só: os cidadãos não possuem ciência do que ocorre com o seus dados, quais as possibilidades de interconexão presente na *internet*, assim como os riscos e consequências futuras que advirão do seu processamento (HOFFMANN-RIEM apud MENDES, 2014). Apenas aceitam as cláusulas impostas para usufruir produtos e serviços em troca de seus dados pessoais[35], a exemplo dos contratos de adesão nas relações consumeristas, que também compõem o âmbito de proteção do novel direito fundamental proposto. Nesse contexto, a perda de controle sobre os próprios dados gera um dever de proteção estatal, sendo necessária a atuação do poder público no tocante ao consentimento meramente aparente do indivíduo[36], (MENDES, 2014).

Nacional de Proteção de Dados Pessoais e da privacidade; fiscalização e aplicação de sanções em caso de tratamento de dados realizado em descumprimento à legislação, por meio de processo administrativo que assegure o direito ao contraditório, ampla defesa e direito de recurso; apreciação de petições dos titulares dos dados pessoais, quando comprovada a não solução do problema pelo controlador; promoção do conhecimento à população das normas e políticas públicas ligadas à proteção de dados pessoais; promoção e elaboração de estudos acerca das práticas nacionais e internacionais de proteção de dados; promoção de ações de cooperação com autoridades de proteção de dados pessoas de outros países; realização de auditorias, quando da realização de sua atividade de fiscalização; aplicação de sanções administrativas e cíveis, dentre outras (BRASIL, 2018).

[35] Indicação de leitura: ROMERO, Luiz. *Não li e concordo.* Disponível em: https://super.abril.com.br/tecnologia/nao-li-e-concordo/. Acesso em: 30 nov. 2019. De acordo com Bruno Bioni, "a coleta dos dados pessoais é contínua. Na medida em que se usufrui de um produto ou serviço, várias informações estão sendo coletadas e agregadas, sendo incerto o fluxo informacional e o que deles se pode extrair. Ainda que seja paradoxal, compra-se agora para pagar depois" (BIONI, 2019, p. 28).

[36] Pensando justamente no consentimento do titular, a LGPD, principal norma acerca da proteção de dados pessoais no território brasileiro atualmente, prevê que: o consentimento deve ser extraído por meio de "cláusulas contratuais destacadas" (art. 8º, §1º), autorizações genéricas, sem finalidade determinada, serão consideradas nulas (art. 8º, §4º), e o consentimento deve ser fornecido por escrito ou por meio que demonstre a manifestação de vontade do titular (art. 8º) (BRASIL, 2018). É nesse contexto que a palavra "consentimento" aparece trinta e cinco vezes no texto da LGPD (BIONI, 2019), em contraponto com o Código de Defesa do Consumidor, em que tal expressão não é sequer

Os deveres de proteção envolvem, inclusive, uma perspectiva relacionada à proibição da proteção insuficiente dos dados pessoais. Assim, tanto a intervenção indevida do Estado na esfera do indivíduo quanto a não atuação, ou atuação insuficiente, gerariam violações ao direito (MENDES, 2014) que, aqui, se entende por fundamental. Devem os poderes públicos, portanto, tutelar de forma suficiente e adequada a proteção de dados pessoais, sendo a proibição da proteção insuficiente uma face do princípio da proporcionalidade (NOVELINO, 2016).

Ademais, pelo fato do direito à proteção de dados ser considerado fundamental, está sujeito a limitações, devido à necessidade de conciliação com outros direitos e bens constitucionalmente protegidos. De acordo com Laura Mendes, existem alguns critérios a serem observados para tal restrição, podendo-se citar como exemplo: a necessidade de determinado processamento para um fim legítimo tutelado pelo ordenamento jurídico; para o cumprimento de direito de terceiro ou, ainda, quando observada a pertinência temática entre o tratamento e a finalidade a ser atingida (MENDES, 2014). Tais hipóteses são elencadas na Lei Geral de Proteção de Dados em seu art. 7º, incisos II, III, IV, V, VI, VII, VIII, IX e X[37], que preveem as situações em que o tratamento de dados poderá ser realizado, ainda que, sem o consentimento do titular.

Dessa forma, o empregador tem o direito de requisitar demandar do empregado dados pessoais aptos a comprovar as habilidades para o cargo. Ocorre que, a exigência de certidões negativas de débito emitidas pelos serviços de

---

mencionada. Já no Marco Civil da Internet, legislação que antecedeu a LGPD, a expressão aparece apenas três vezes. Parece-nos que tal fato demonstra o amadurecimento do legislador em considerar a importância da decisão do indivíduo quando do tratamento de seus dados pessoais.

[37] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
[...]
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (BRASIL, 2018).

proteção ao crédito, por exemplo, mostrar-se-ia desarrazoada, já que tal informação é desnecessária para certificar a capacidade laboral do trabalhador e diz respeito a relações consumeristas. Ademais, a transferência de dados pessoais presentes no banco de dados do programa federal Bolsa-Família para outros órgãos do governo pode ser necessária para o cumprimento de políticas públicas e realização de programas sociais. Entretanto, a transferência desses dados sensíveis ao setor privado pode demonstrar-se descontextualizada, uma vez que a divulgação de informações acerca da situação financeira dos beneficiados pode ocasionar estigmatização e discriminação dentro da sociedade (MENDES, 2014).

Merece destaque, ainda, o fato de que a Corte Constitucional alemã vem afirmando, com frequência, a existência de um "núcleo absolutamente protegido" ("*absolut geschutzter Kernbereich privater Lebensgestaltung"*)[38] de tal direito, insuscetível de restrições e interferências. A questão, contudo, é controversa, sendo difícil o estabelecimento de um núcleo essencial do direito à proteção de dados (MENDES, 2014).

Fato é que a utilização de dados pessoais, na atual sociedade da informação, é imprescindível para o aperfeiçoamento de diversas relações sociais, sendo o seu fornecimento a porta de entrada para a obtenção de diversos produtos e serviços. Como bem exposto por Mayer-Schonberger, "somente os eremitas alcançariam a proteção plena de seus dados, já que, como decorrência da sua recusa em fornecê-los, amargariam o custo social decorrente da exclusão de tais atividades" (BIONI, 2019, p. 116).

4.3 PROPOSTA DE EMENDA CONSTITUCIONAL 17/2019

A recente aprovação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) ampliou sobremaneira a discussão acerca do tema no país. Sabe-se que todos os âmbitos da vida são marcados pelo processamento de dados pessoais e que essa utilização é imprescindível para o oferecimento de bens e serviços - públicos e privados - na sociedade. À vista disso, foi aprovada em julho de 2019, no plenário do Senado Federal, a proposta de Emenda à Constituição nº 17, a qual possui como

[38] "Área central absolutamente protegida da vida privada" (*Tradução nossa*).

objetivo primordial acrescentar o inciso XII-A ao artigo 5º, bem como o inciso XXX ao artigo 22 da CRFB/88 (BRASIL, 2019).

Caso aprovada, sem mais alterações, nos demais turnos, os dispositivos supracitados passarão a vigorar com a seguinte redação:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País, a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.
> [...]
> Art. 22. Compete privativamente à União legislar sobre:
> [...]
> XXX – proteção e tratamento de dados pessoais.

Dentre as justificativas para a alteração constitucional, tem-se que a proteção de dados é fruto da evolução histórica da sociedade internacional, uma vez que o seu tratamento indevido representa riscos às liberdades e garantias dos cidadãos. O direito à privacidade configurou-se como verdadeiro ponto de partida de diversas discussões e regulações, já se vislumbrando, no entanto, grande autonomia e diversas peculiaridades, bem como diferentes amplitude e abrangência, do direito à proteção de dados em relação àquele, merecendo-se tornar um direito constitucionalmente assegurado (BRASIL, 2019).

Ainda, a justificação da PEC 17/2019 dispõe que o Brasil necessita muito mais do que uma lei ordinária acerca do assunto, entendimento também compartilhado pelo presente trabalho. A existência de uma norma constitucional expressa sobre o tratamento de dados pessoais propiciará maior segurança jurídica aos indivíduos, que saberão exatamente o conteúdo abarcado pelo novo direito, assim como as restrições a que esse está sujeito. Nesse mesmo sentido, a previsão específica para a proteção de dados resultará em uma proteção mais ampla, impedindo violações do próprio legislador, que deverá observar tal direito fundamental quando da edição de novas leis. A LGPD, portanto, não está apta a tutelar os indivíduos de outras normas que, porventura, venham a ser aprovadas pelo Poder Legislativo e que prevejam o processamento indevido de dados, a legitimação de práticas de vigilância (MENDES, 2019), a coleta ilimitada, dentre outros aspectos que podem ser facilmente protegidos com a previsão constitucional.

Há, no entanto, opiniões em sentido contrário. Anderson Schreiber (2019), em uma análise crítica ao jornal online Carta Forense[39], afirma que a proposta de inclusão da proteção de dados no rol de direitos fundamentais possui mero valor simbólico, concluindo que a PEC 17/2019 é desnecessária e, até mesmo perigosa. Isso porque, segundo o autor, a proteção de dados pessoais já vem sendo extraída pela doutrina e jurisprudência a partir de outras normas constitucionais explícitas, como, por exemplo, do direito à privacidade (art. 5º, X) e da cláusula geral da dignidade da pessoa humana (art. 1º, III).

Em relação à alteração proposta pela PEC ao artigo 22 da CFRB/88, afirma que a competência privativa da União para legislar sobre o tema pode ir de encontro ao propósito central da PEC, uma vez que, em vez de ampliar a proteção, traz o risco de limitá-la. Nesse contexto, pelo fato de a disciplina do tema envolver uma série de formas de tratamento de dados (coleta, produção, recepção, utilização, acesso, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, entre outros), restringir a atuação legislativa a apenas uma entidade federativa é capaz de diminuir a proteção da matéria, podendo, inclusive, comprometer a validade de normas estaduais que já são aplicadas como importantes instrumentos de tutela (SCHREIBER, 2019).

Assim, traz o autor algumas normas estaduais dos estados do Rio de Janeiro[40] e São Paulo[41] que são voltadas para o direito do consumidor, mas, reflexamente, protegem dados pessoais de utilizações indevidas. Tais leis, que foram editadas no exercício da competência concorrente, podem futuramente vir a ser consideradas inconstitucionais, caso se entenda que a matéria principal vinculadas por elas é o tratamento de dados e não os direitos dos consumidores em si. Dessa forma, afirma que:

> Ao restringir a competência legislativa para o tratamento de dados pessoais à União, a PEC 17/2019 lançaria uma sombra de dúvida sobre a constitucionalidade dessas e outras tantas leis estaduais, que já exercem importante papel na tutela da autodeterminação informacional da pessoa humana. (SCHREIBER, 2019).

Ademais, a competência legislativa privativa da União pode gerar certa dificuldade de atuação da Autoridade Nacional de Proteção de Dados (ANPD),

[39] Disponível em: http://www.cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345. Acesso em: 28 nov. 2019.
[40] Lei nº 4.896/2006 do Estado do Rio de Janeiro.
[41] Lei nº 13.226/2008 do Estado de São Paulo.

criada pela LGPD e que possui como uma de suas atribuições “editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade” (SCHREIBER, 2019). O poder de produção normativa da referida entidade administrativa é essencial “para dar concretude e efetividade aos dispositivos por vezes demasiadamente genéricos da LGPD” (SCHREIBER, 2019), afirmando o autor, ainda, que:

> Qualquer coisa que possa servir como argumento contra o poder normativo da Autoridade Nacional de Proteção de Dados deve ser vista com muita cautela, pois pode comprometer sua atuação eficaz na realidade brasileira. Uma previsão de competência privativa da União para legislar sobre o tema da proteção de dados pessoais pode, nesse sentido, reforçar preconceitos e criar “reservas” de produção normativa que não contribuirão para a consolidação de uma cultura de proteção de dados pessoais em nossa sociedade. (SCHREIBER, 2019).

A justificação trazida pela PEC 17/2019 para tal locus é no sentido de que deve ser evitada a fragmentação e pulverização de um tema caro à sociedade como a proteção de dados. Do contrário, surgiria o risco de existirem os mais variados conceitos acerca de “dados pessoais” e “agentes de tratamento”, por exemplo. A proposta afirma, ainda, que é praticamente inviável às empresas se adaptarem aos mais diversos diplomas normativos específicos de cada localidade, devendo o país apresentar uma legislação uniforme quanto ao tema (BRASIL, 2019). Nesse contexto, empresas nacionais e estrangeiras, que possuem como uma de suas atividades – ou até mesmo a principal - o tratamento de dados pessoais, encontrariam maiores facilidades quando da realização de negócios e investimentos no território brasileiro, já que não existiriam diversas normas estaduais e municipais sobre o tema.

Tal controvérsia, contudo, não inviabiliza a necessidade de reconhecimento do caráter autônomo do direito à proteção de dados, somente restando dúbio se sua disciplina deverá ficar situada em sede do art. 22 da CRFB/88 (competência legislativa privativa da União) ou do art. 24 (no âmbito da competência concorrente), a fim de harmonizar-se com as disciplinas consumeristas já existentes.

Para o presente trabalho, a previsão constitucional é primordial para a defesa dos indivíduos quanto ao tratamento dos seus dados. Parece-nos que o tema ora abordado está em constante amadurecimento, devendo a questão ser tratada com, cada vez mais, responsabilidade, já que as informações pessoais viraram verdadeira

moeda de troca na sociedade. Como afirmado, a previsão de tal direito no rol de direitos fundamentais geraria maior segurança jurídica aos cidadãos, que estariam mais particularmente protegidos contra a edição de novas leis e mudanças de interpretações e entendimentos do Poder Judiciário.

5 CONSIDERAÇÕES FINAIS

No decorrer do presente trabalho foram discutidos aspectos relacionados à sociedade da informação, privacidade, proteção de dados e aos direitos fundamentais. Primeiramente, buscou-se demonstrar como é realizada a vigilância sobre os indivíduos na atual era informacional, possibilitada pelo advento de diversos aparatos tecnológicos que permitiram a utilização intensa de informações pessoais para as mais variadas finalidades.

Em um segundo momento, discutiram-se os principais conceitos, princípios e normas que regulam os dados/informações pessoais dos indivíduos, aspectos esses essenciais para a compreensão do tema ora abordado. Verificou-se que existem diversos princípios que devem, obrigatoriamente, ser observados quando do processamento de dados pessoais, uma vez que funcionam como verdadeiro norte para os agentes de tratamento e concretizam diversos direitos já previstos no ordenamento como, por exemplo, a dignidade da pessoa humana, privacidade, intimidade, publicidade, informação, dentre outros. Ademais, observou-se que algumas normas internacionais serviram de exemplo para a criação de um regramento próprio no direito brasileiro, demonstrando que o país está seguindo a tendência mundial de tutelar os dados pessoais de forma cada vez mais contundente e específica. A evolução legislativa que culminou na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e, mais recentemente, na PEC 17/2019 demonstra o amadurecimento da visão do legislador e, até mesmo, da sociedade quanto à importância e necessidade de se discutir sobre dados, tecnologia e direito.

Buscou-se, por conseguinte, cotejar os principais direitos fundamentais envolvidos, trazendo-se exemplos concretos de como a utilização indevida de dados pode acarretar riscos e danos imensuráveis aos cidadãos. Constatou-se que a criação de bancos de dados pode se valer de informações que, nem sempre, são consideradas íntimas ou privadas, demonstrando-se que o âmbito de proteção dos dados vai além do que o direito fundamental à privacidade – e outros direitos fundamentais individualmente considerados - é capaz de abarcar. Traçaram-se, portanto, as principais características desse novo direito que se entende por fundamental, bem como as limitações a que está sujeito.

Ainda nesse contexto, foi constatado que o consentimento do titular passou a figurar em posição de extrema relevância para o ordenamento jurídico, devendo ser livre, informado, específico e expresso, ainda que questionável o modo de coleta e efetivação deste na prática. O dever de proteção e cuidado dos agentes de tratamento permanece, uma vez que consentimento formal, aparentemente informado, nem sempre é efetivamente esclarecido. Assim, deve existir a preocupação constante dos Poderes Públicos em elevar o titular a uma posição de destaque e protagonismo quando do tratamento de seus dados, na tentativa de propiciar um verdadeiro direito à autodeterminação informacional.

Nesse sentido, reportou-se ao recente Projeto de Emenda Constitucional nº 17/2019, que pretende incluir no rol de direitos fundamentais do artigo 5º o inciso XII-A, assim como o inciso XXX no artigo 22 da CRFB/88. A PEC tem por objetivo prever o direto à proteção de dados pessoais como um direito fundamental autônomo, desvinculado do direito à privacidade, e a competência privativa da União para legislar acerca da matéria, em que pese a dúvida acerca dessa última disciplina. A proposta corrobora, portanto, o quanto exposto até o presente momento, uma vez que as reflexões aqui delineadas buscam evidenciar o surgimento de um novo direito fundamental específico no seio da sociedade: o direito à proteção de dados pessoais.

Dessa forma, diante da revolução tecnológica vivenciada pelo homem nas últimas décadas, tem-se que os ordenamentos jurídicos devem acompanhar as mudanças sociais, como forma de se manterem atualizados e aptos a proteger os cidadãos dos mais variados riscos existentes. Percebe-se que o direito brasileiro muito evoluiu nos últimos anos no que concerne à proteção do indivíduo diante de novas tecnologias. Tal progresso, no entanto, deve ser ininterrupto, de forma a propiciar a mudança da Constituição e a sua constante atualização, o que, ora se defende, com o reconhecimento do caráter autônomo da proteção de dados como direito fundamental.

REFERÊNCIAS BIBLIOGRÁFICAS

BESSA, L. R. A abrangência da disciplina conferida pelo código de defesa do consumidor aos bancos de proteção ao crédito. In: NERY JÚNIOR, N.; NERY, R. M. D. A. **Coleção doutrinas essenciais:** Responsabilidade Civil - direito à informação. São Paulo: Revista dos Tribunais, v. v 8, 2010. p. 393-438.

BESSA, L. R. **Cadastro Positivo:** comentários à Lei 12.414 de 09 de junho de 2011. São Paulo: Revista dos Tribunais, 2011.

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

BLUM, R. O.; ARANTES, C. R. Autoridades de controle, atribuições e sanções. In: MALDONADO, V. N.; BLUM, R. O. **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 227-252.

BRASIL, Constituição (1988). *Constituição da República Federativa do Brasil.* Brasília, DF: Senado, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ constituicaocompilado.htm>. Acesso em: 15 set. 2019.

CARVALHO, A. C. A. P. **Marco Civil da Internet no Brasil:** Análise da Lei 12.965/14 e do Direito de Informação. Rio de Janeiro: Alta Books, 2014.

CASTELLS, M. **A sociedade em rede**. Tradução de Roneide Venâncio Majer. 8. ed. São Paulo: Paz e Terra, v. 1, 2000.

CHAVES, L. F. P. Responsável pelo tratamento, subcontratante e DPO. In: MALDONADO, V. N.; BLUM, R. O. **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 111-138.

CHILE, CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE. 1980. MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA. Disponível em: https://www.leychile.cl/Navegar?idNorma=242302&idParte=&idVersion=&r=1. Acesso em: 28 nov. 2019.

COSTA, C. C. O. D. **Cadastro Positivo:** Lei n. 12.414/2011 comentada artigo por artigo. São Paulo: Saraiva, 2012.

COSTA, C. L. J.; FERES JÚNIOR, J. Carta Maior. **Racial profiling e direitos do cidadão:** as contradições de uma política de segurança pública racista, 29 set. 2015. Disponivel em: <https://www.cartamaior.com.br/?/Editoria/Direitos-

Humanos/Racial-profiling-e-direitos-do-cidadao-as-contradicoes-de-uma-politica-de-seguranca-publica-racista/5/34623>. Acesso em: 25 nov 2019.

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

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, p. 91-108. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658. Acesso em: 28 ago 2019.

DOTTI, R. A. **Proteção da Vida Privada e Liberdade de Informação**. São Paulo: RT, 1980.

FARIAS, Cyntia Mirella da Costa; CANDIDO, Nathalie Carvalho. Medicina preditiva e biodireito. In: ENCONTRO NACIONAL DO CONPEDI, 19., 2010, Fortaleza. **Anais eletrônicos...** Florianópolis: Fundação Boiteux, 2010. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/fortaleza/3463.pdf >. Acesso em: 20 nov. 2019.

FERRAZ JÚNIOR, T. S. Sigilo de dados: O direito à privacidade e os limites da função fiscalizadora do estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, 1993. 430-459.

FOUCAULT, M. **Vigiar e Punir:** nascimento da prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987.

GENERAL DATA PROTECTION REGULATION EU. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 10 out. 2019.

JESUS, D. D.; MILAGRE, J. A. **Marco Civil da Internet:** comentários à Lei n. 12.965 de 23 de abril de 2014. São Paulo: Saraiva, 2014.

JIMENE, C. D. V. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, V. N.; BLUM, R. O. **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 169-184.

LACE, S. **The glass consumer:** life in a surveillance society. Bristol: Policy Press, 2005.

LÉVY, P. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

_____. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da República Federativa do*

Brasil, Brasília, DF, 12 de setembro de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L8078.htm >. Acesso em: 30 set. 2019

_____. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. *Diário Oficial da República Federativa do Brasil,* Brasília, DF, 12 de novembro de 1997. Disponível em: <http://www.planalto.gov.br /ccivil_03/leis/L9507.htm>. Acesso em: 10 mai. 2016.

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da República Federativa do Brasil,* Brasília, DF, 14 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 set 2019.

LIMA, C. C. C. Objeto, Aplicação Material e Aplicação Territorial. In: MALDONADO, V. N.; BLUM, R. O. **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters, 2018. p. 23-36.

MARQUES, G.; MARTINS, L. **Direito da Informática**. Coimbra: Almedina, 2006.

MELO, J. O. D. Consultor Jurídico. **Segurança Nacional:** FBI considera todos culpados em sua lista, 2011b. Disponivel em: <https://www.conjur.com.br/2011-set-29/fbi-considera-todos-culpados-lista-mesmo-prove-contrario>. Acesso em: 20 nov 2019.

MELO, J. O. D. Consultor Jurídico. **Nos EUA, lista de suspeitos de terrorismo viola direitos constitucionais**, 2019a. Disponivel em: <https://www.conjur.com.br/2019-set-10/eua-lista-suspeitos-terrorismo-viola-direitos-constitucionais#top>. Acesso em: 20 nov 2019.

MENDES, L. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Panorama Setorial da Internet**, n. 2 ed., Junho 2019. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano-xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: 10 set 2019.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor:** linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MORAES, A. D. **Direito Constitucional**. 34. ed. São Paulo: Atlas, 2018.

_____. *O projeto genoma humano,* 2001. Disponivel em: <http://genoma.ib.usp.br/sites/default/files/projeto-genoma-humano.pdf>. Acesso em: 25 nov 2019.

OLIVEIRA, B. P. G.; LAZARI, R. D. **Manual de direitos humanos:** volume único. Salvador: Juspodivm, v. 3 rev., ampl. e atual., 2017.

PAESANI, L. M. **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

PENA, S. D.; AZEVEDO, E. S. O projeto Genoma Humano e a Medicina Preditiva: Avanços técnicos e dilemas éticos. In: COSTA, S. T. F.; OSELVA, G.; GARRAFA, V. **Iniciação à Bioética**. Brasília: Conselho Federal de Medicina, 1998.

PEZZI, A. P. J. **A necessidade de proteção dos dados pessoais nos arquivos de consumo:** em busca da concretização do direito à privacidade. Tese (Mestrado). São Leopoldo: Universidade do Vale do Rio dos Sinos, 2007.

PINHEIRO, P. P. **Direito digital aplicado 3.0**. 1. ed. São Paulo: Thomson Reuters Brasil, 2018.

PORTUGAL. Texto originário da Constituição, aprovada em 2 de Abril de 1976. **Constituição da República Portuguesa.** Lisboa, Portugal, 2 abr. 1976**.** Disponível em: <http://www.parlamento.pt/parlamento/documents/crp1976.pdf>. Acesso em: 25 nov. 2019

RAMOS, A. D. C. O pequeno irmão que nos observa: os direitos dos consumidores e os bancos de dados no Brasil. In: MARQUES, C. L.; MIRAGEM, B. **Coleção doutrinas essenciais:** direito do consumidor - proteção da confiança e práticas comerciais. São Paulo: Revista dos Tribunais, v. 3, 2011. p. 957-974.

RODOTÁ, S. **A vida na sociedade da vigilância**. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, I. W.; MARINONI, L. G.; MITIDIERO, D. **Curso de Direito Constitucional**. 7. ed. São Paulo: Saraiva, 2018.

SCHREIBER, A. Jornal Carta Forense. **PEC 17/19:** Uma Análise Crítica, 2019. Disponivel em: <http://www.cartaforense.com.br/conteudo/colunas/pec-1719-uma-analise-critica/18345>. Acesso em: 28 nov 2019.

SILVA, D. P. M. **Desafios do ensino jurídico na pós-modernidade:** da sociedade agrícola e industrial para a sociedade da informação. Dissertação (Mestrado). São Paulo: Faculdade de Direito da Pontifícia Universidade Católica de São Paulo, 2009. Acesso em: 15 Setembro 2019.

SILVA, M. A. C. D. **A RECONSTRUÇÃO CONTEMPORÂNEA DA NOÇÃO DE PRIVACIDADE, O MARCO CIVIL DA INTERNET E O PROJETO DE LEI DE PROTEÇÃO DE DADOS PESSOAIS**. Salvador: UNIVERSIDADE FEDERAL DA BAHIA. Tese (Graduação), 2016. 177 p.

SIQUEIRA JR, P. H. **Teoria do Direito**. São Paulo: Saraiva, 2012.

TAKAHASHI, T. **Sociedade da informação no Brasil:** livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TEIXEIRA, T. **Marco Civil da Internet:** comentado. São Paulo: Almedina, 2016.

UNIÃO EUROPEIA. 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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 10 out 2019.

VAINZOF, R. Dados pessoais, tratamento e princípios. In: MALDONADO, V. N.; BLUM, R. O. **Comentários ao GDPR:** Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018. p. 37-84.

VAINZOF, R. Capítulo I - Disposições Preliminares. In: MALDONADO, V. N. (.).; BLUM, R. O. (.). **LGPD:** Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2019. p. 19-178.

VIANA, R. C. L. **Pode o empregador ter acesso à informação genética do trabalhador?** São Paulo: LTR, 2013.

VIEIRA, T. M. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado). Brasília: Universidade de Brasília, 2007.

WILLEMIN, A. Consultor Jurídico. **A importância do avanço nas leis de proteção de dados**, 28 jan 2019. Disponivel em: <https://www.conjur.com.br/2019-jan-28/opiniao-importancia-avanco-leis-protecao-dados>. Acesso em: 20 nov 2019.

ZATZ, M. **Projeto genoma humano e ética**. São Paulo Perspec. São Paulo, v. 14, n. 3, 2000. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-88392000000300009&lng=en&nrm=iso>. Acesso em: 25 nov. 2019.