INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA (IDP)
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL

JOSILENNI DE ALENCAR FONSECA SANTOS

A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL NO BRASIL: UMA ANÁLISE DA SUA FUNDAMENTALIDADE MATERIAL PARA A CONSTRUÇÃO DE UMA ESTRUTURA DOGMÁTICA

TERESINA - PI
2021

JOSILENNI DE ALENCAR FONSECA SANTOS

A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL NO BRASIL: UMA ANÁLISE DA SUA FUNDAMENTALIDADE MATERIAL PARA A CONSTRUÇÃO DE UMA ESTRUTURA DOGMÁTICA

Dissertação apresentada ao Programa Interinstitucional de Pós-Graduação *Stricto Sensu* do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) como requisito para a obtenção do título de mestre em Direito Constitucional

Orientadora: Profª Dra. Laura Schertel Mendes

TERESINA - PI

2021

JOSILENNI DE ALENCAR FONSECA SANTOS

A PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL NO BRASIL: UMA ANÁLISE DA SUA FUNDAMENTALIDADE MATERIAL PARA A CONSTRUÇÃO DE UMA ESTRUTURA DOGMÁTICA

Dissertação apresentada ao Programa Interinstitucional de Pós-Graduação *Stricto Sensu* do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) como requisito para a obtenção do título de mestre em Direito Constitucional

Orientadora: Profª Dra. Laura Schertel Mendes

Aprovada em: _____, _____de _____.

BANCA EXAMINADORA

_____

Profa. Dra. Laura Schertel Mendes (orientadora) - IDP

_____

Prof. Dr. Danilo Cesar Maganhoto Doneda - IDP

_____

Prof. Dr. Leandro Cardoso Lages - UFPI

AGRADECIMENTOS

Seria impossível atravessar esse caminho sozinha, principalmente em meio a uma pandemia que assolou todo o mundo, que, além de perdas de valor inestimável, trouxe para nossas vidas um mar constante de incertezas e medo do futuro, numa saturação de sentimentos que por vezes nos levou a um verdadeiro esgotamento mental e físico.

Não foi fácil. Por isso, busquei sempre a companhia de Deus, a quem agradeço todos os dias por me manter viva e saudável, juntamente com meus familiares, e por me dar forças sempre que fraquejava ou pensava em desistir.

A realização desse sonho também só foi possível com o apoio incondicional da minha mãe, Maria Elita, que me cercou de todo amor possível e palavras de incentivo, e mesmo não tendo tido a oportunidade de fazer um curso superior, sempre me mostrou que a educação era o melhor caminho a trilhar.

Agradeço ainda a todos os meus amigos, pela compreensão e suporte emocional nessa fase de distanciamento, ao Prof. Dr. Nestor Alcebíades Mendes Ximenes, pela oportunidade de desenvolvimento profissional e pelo apoio de sempre, e aos professores membros dessa banca, em especial o Prof. Dr. Danilo Cesar Maganhoto Doneda e o Prof. Dr. Leandro Cardoso Lages, pela disposição em participar da avaliação desse trabalho.

Por fim, agradeço à minha orientadora, Prof.ª. Dra. Laura Schertel Mendes, que me descortinou o mundo da proteção de dados, com a sugestão do tema e suas valorosas lições. Tornei-me uma entusiasta da matéria e uma grande admiradora do seu trabalho na área.

"*A unidade da pessoa está fragmentada. [...] Cada um de nós está presente em dezenas de bancos de dados*".

Stefano Rodotà

RESUMO

Essa dissertação propõe uma análise da fundamentalidade material do direito à proteção de dados pessoais no Brasil, com vistas a justificar a sua possível categorização como um direito fundamental implícito na Constituição Federal, conforme autorização prevista no art. 5º, § 2º, dessa Carta. Com a utilização de parâmetros extraídos de normas constitucionais bem como das posições jurídicas deduzidas da Lei 13.709/2018, busca-se averiguar o conteúdo, a importância e o âmbito de proteção desse direito fundamental implícito e assim contribuir para os primeiros contornos da sua estrutura dogmática, apresentando, ainda, a visão dos Tribunais pátrios, especialmente do Supremo Tribunal Federal, sobre o tema.

Palavras-chave: Direitos fundamentais. Fundamentalidade material. Estrutura dogmática. Privacidade. Proteção de dados.

ABSTRACT

This dissertation proposes an analysis of the material fundamentality of the right to personal data protection in Brazil, with a view to justifying its possible categorization as a fundamental right implicit in the Federal Constitution, as authorized by art. 5, § 2, of this Letter. With the use of parameters extracted from constitutional norms as well as the legal positions deduced from Law 13.709 / 2018, it is intended to investigate the content, the importance and the scope of protection of this implicit fundamental right and, this way, contribute to the first contours of its dogmatic structure, also presenting the view of the Brazilian Courts, especially the Federal Supreme Court, on the subject.

Keywords*:* Fundamental rights. Material fundamentality. Dogmatic structure. Privacy. Data protection.

SUMÁRIO

1 INTRODUÇÃO

A discussão a respeito da proteção de dados pessoais nunca foi tão necessária, principalmente na atual fase tecnológica em que a sociedade se encontra, em que a informação acabou se tornando um bem de grande valor.

Isso porque o aumento exponencial do uso das tecnologias da informação provocou, ao longo do tempo, a ampliação também do fluxo de informações e da coleta de dados pessoais, que, por sua vez, transformaram-se num verdadeiro fator de competitividade e desenvolvimento tanto na economia nacional como na internacional.

Por consequência, esse fenômeno chamou a atenção do legislador e de juristas de todo o mundo, uma vez que a preocupação com a proteção dos dados pessoais e com as formas de blindagem do cidadão quanto ao armazenamento desses dados, por parte de empresas públicas e privadas, tornou-se um ponto nevrálgico do universo jurídico.

Ao longo dos anos, com a eclosão de diversos diplomas legais sobre o tema, buscou-se assegurar, diante do inevitável progresso tecnológico, a intimidade e a liberdade dos indivíduos, apresentando-se a proteção de dados pessoais como mais uma das facetas da privacidade, a qual teve seu conceito e amplitude modificados em razão dos estudos sobre o tema.

No entanto, por muito tempo, a privacidade que, para alguns autores, é considerada gênero do qual o direito à intimidade e o direito à vida privada são espécies, não foi uma preocupação da grande maioria das pessoas, sendo, inclusive, a sua noção desconhecida pelos povos antigos, uma vez que os seus cotidianos se transcorriam nos espaços públicos. Isso fez com que a ideia de vida privada e de intimidade fosse sentida de formas bem diferentes, de acordo com a sociedade de cada época, tendo em vista suas dimensões política e econômica e o fato de a noção de público e privado evoluir de forma interna em cada indivíduo, como forma de expressão da sua personalidade.

A construção da privacidade enquanto direito só aconteceu no final do século XIX, com as transformações socioeconômicas da revolução industrial e quando a burguesia se solidificou como classe social. Ele acabou se tornando um direito de fato autônomo, merecendo estudos e doutrina voltada para sua proteção após o seu reconhecimento pela Declaração Universal de Direitos Humanos de 1948[1] (ONU, 1948), quando passou a ser enquadrado na categoria de direitos humanos e, posteriormente, de direitos fundamentais, com a sua constitucionalização.

[1] Somente no final do século XIX, o direito à privacidade surge como figura jurídica autônoma e se torna parte da ordem jurídica, expandindo-se à sociedade em geral. Colaborou para esse fenômeno a sua internalização pela Declaração Universal dos Direitos Humanos, proclamada pela Organização das Nações Unidas (ONU), que em

Esse fenômeno foi motivado ainda pelo avanço da tecnologia e pelo crescimento da circulação de informações, as quais se tornaram mais fáceis de serem recolhidas, processadas e utilizadas, levando a uma crescente preocupação da sociedade com a vida privada e a intimidade e promovendo a democratização do interesse pela tutela de tais direitos bem como de seu exercício. Desde então, constatou-se uma rápida evolução do direito à privacidade, que, após ser reconhecido no plano internacional, aos poucos foi incorporando-se ao ordenamento jurídico interno de cada país.

Ressalta-se, entretanto, que a tutela da privacidade só passou a ser objeto de reflexões mais profundas recentemente, em razão das transformações sociais advindas da revolução tecnológica[2], no século XX, em decorrência, especialmente, do surgimento da Internet e das suas ferramentas de comunicação, que inseriu a sociedade num ambiente virtual e propiciou uma maneira diferente de interação das pessoas com o mundo, produzindo uma nova forma de lidar com a noção de privado.

Com isso, a informação assumiu cada vez mais relevância, deixando de se restringir ao ambiente privado e ganhando expressiva visibilidade, ascendendo ao posto de principal riqueza com as novas tecnologias digitais, que permitiram o seu processamento e a sua transmissão em quantidade e velocidade nunca imaginada, numa transposição de barreiras territoriais e temporais.

Esse fenômeno abriu espaço, ainda, para o surgimento dos bancos de dados, possibilitando a coleta, a produção, a transmissão e o armazenamento de dados diversos[3], inclusive aqueles relativos à vida pessoal dos indivíduos, fazendo com que a manipulação da informação pessoal ganhasse proeminência na sociedade e daí emergissem conflitos e violações de direitos fundamentais como a privacidade, influenciando diretamente na seara jurídica.

Essa nova realidade acabou ressignificando o conceito de privacidade, que antes consistia numa liberdade negativa, no sentido de preservar o indivíduo do poder do Estado, e ganhou um aspecto positivo, no momento em que esse mesmo indivíduo passou a requerer prestações do Estado com vistas a garantir o exercício desse direito, já que o aumento do fluxo

---

seu art. XII, prevê: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

[2] Manuel Castells pontua que, na década de 1970, surgiu um novo paradigma tecnológico, organizado com base na tecnologia da informação constituído, principalmente, nos Estados Unidos. Segundo ele, "[...] foi um segmento específico da sociedade norte-americana, em interação com a economia global e a geopolítica mundial, que concretizou um novo estilo de produção, comunicação, gerenciamento e vida" (CASTELLS, 2019, p. 698).

[3] "Hoje, com o desenvolvimento da informática, armazenam-se um número ilimitado de dados de todas as naturezas, os quais circulam entre Estados, particulares e empresas privadas, muitas vezes sem qualquer tipo de controle" (RAMINELLI; RODEGHERI, 2016, p. 91).

de informações modificou, paulatinamente, os meios "clássicos" de violações da privacidade, que se tornou mais frágil e exposta a ameaças.

Assim, com o habitual processamento massivo de informações, deixou-se de tratar da privacidade com o mesmo parâmetro que ela representou para outras sociedades (DONEDA, 2019), principalmente após o surgimento de computadores, em seguida, dos bancos de dados e do controle sobre a informação – em especial, dos dados pessoais[4] – que passou a ser visto como uma nova forma de poder (VERGILI, 2019), utilizada tanto pela atividade empresarial como pelo setor público.

Hoje, com o desenvolvimento de potentes *softwares*, tornou-se fácil o acesso, o armazenamento e a alteração de dados pessoais, bem como a manipulação dessas informações em grande escala através de técnicas sofisticadas que permitem empreender de forma mais eficiente no mercado[5], ajudando a direcionar, por exemplo, mensagens publicitárias personalizadas, de acordo com o perfil identificado.

Os dados pessoais ganharam, assim, posição central no universo digital, reinventando, por isso, o conceito de privacidade. Por essa razão, "a tutela da privacidade passou a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada" (MULHOLLAND, 2012, p.3), originando, assim, o direito à proteção de dados, que começou a receber tutela específica em diversos ordenamentos jurídicos, sendo reconhecido, inclusive, como um direito fundamental por diversos países.

Isso porque os dados passaram a ser vistos como uma projeção da própria personalidade do indivíduo, sendo quase impossível dissociar a sua proteção com a tutela de outros direitos fundamentais, tais como a privacidade, a intimidade, a liberdade, dentre outros, o que fez com que o direito à proteção de dados passasse a ser compreendido sob uma ótica também constitucional.

No Brasil, não são raros os entendimentos nesse sentido, principalmente após o advento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que entrou em vigor em agosto de 2020, trazendo um regime próprio de princípios, direitos, obrigações e sanções relacionadas ao

---

[4] Nesse sentido, mostra-se relevante a diferenciação entre dados sensíveis e não-sensíveis. Em relação ao primeiro, entende-se como aqueles referentes à ideologia, religião ou crença, origem racial, saúde ou vida sexual, que, por sua natureza distinta, devem ter especial proteção, a fim de evitar situações de discriminação. Dessa forma, os dados não-sensíveis são, portanto, aqueles não considerados como detentores de especial proteção por não violarem, diretamente, o princípio à igualdade.

[5] Dentre essas técnicas, está a *profiling*, "[...] em que os dados pessoais de um indivíduo formam um perfil a seu respeito para a tomada de inúmeras decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na Internet" (BIONI, 2020, p. 86).

tratamento de dados pessoais que fortaleceu ainda mais a ideia de que o direito à proteção de dados se trata de um direito fundamental, se analisado em conjunto com regras constitucionais.

Não à toa, foi aprovada também recentemente pelo Senado Federal a Proposta de Emenda à Constituição (PEC) 17/2019, que inclui de forma expressa o direito à proteção de dados pessoais no texto constitucional, alterando o artigo 5º, inciso XII, e o artigo 22, inciso XXX, inserindo esse direito na lista de garantias individuais da nossa Carta Magna.

Recentemente, em maio de 2020, essa discussão ganhou ainda mais relevo após decisão paradigmática emanada pelo Supremo Tribunal Federal, nos autos da Ação Direta de Inconstitucionalidade nº 6387 MC/DF, no qual essa Corte reconheceu, pela primeira vez, um direito fundamental à proteção de dados, após suspender a eficácia da Medida Provisória nº 954/2020, que determinava que empresas de telecomunicações prestadoras de Serviço Telefônico Fixo entregassem dados pessoais de seus clientes (nome, endereço e telefone), a fim de que a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) realizasse a Pesquisa Nacional por Amostra de Domicílios (Pnad) Contínua[6], de forma não presencial, durante a pandemia causada pelo Coronavírus.

De acordo com essa decisão, que será melhor explorada no decorrer dessa dissertação, diante dos riscos e as ameaças que envolvem o tratamento de dados, o ato normativo supracitado não deixou clara a sua finalidade, a sua necessidade bem como a certeza de segurança nesse procedimento, o que poderia ensejar violações a direitos como a privacidade, a intimidade e ao livre desenvolvimento da personalidade dos cidadãos brasileiros.

Tais aspectos demonstram, assim, não só a atualidade, mas também a relevância jurídica do tema, justificando o debate proposto no presente estudo, que pretende analisar a fundamentalidade material do direito à proteção de dados, uma vez que ele não está expressamente previsto no rol de direitos fundamentais constantes da nossa Constituição Federal, mas pode ser deduzido do artigo 5º, § 2º, dessa Carta[7], que traz a possibilidade de existência de direitos fundamentais implícitos ou decorrentes, sendo esse o objetivo geral dessa dissertação.

---

[6] A PNAD Contínua é uma pesquisa realizada pelo Instituto Brasileiro de Geografia e Estatística e visa produzir indicadores para acompanhar as flutuações trimestrais e a evolução, a médio e longo prazos, da força de trabalho e outras informações necessárias para o estudo e desenvolvimento socioeconômico do País. É uma pesquisa estatística por amostragem que avalia critérios importantes, como o desemprego, para fins de política macroeconômica (IBGE, 2020).

[7] Aduz esse dispositivo, *in verbis:* "Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte" (Brasil, 1988).

Busca-se, dessa forma, debater se o conteúdo, a importância e o alcance do direito à proteção de dados o tornam um direito fundamental em sentido material a ponto de permitir sua equiparação àqueles que fazem parte do catálogo de direitos fundamentais previstos no art. 5º da Magna Carta. Para tanto, esse estudo propõe delinear a estrutura dogmática desse direito no Brasil, através da análise das posições jurídicas que podem ser extraídas da Lei nº 13.709/2018, e assim contribuir para a definição do seu conteúdo, da sua titularidade, dos seus destinatários bem como de outros elementos que, vistos sob uma ótica constitucional, justificariam a sua fundamentalidade material.

E partindo do pressuposto de que se trata de um direito fundamental implícito, essa dissertação ainda tem como objetivo específico a análise da proteção de dados tanto na sua dimensão subjetiva, se considerado um direito individual oponível ao Estado e aos demais particulares, como também na sua dimensão objetiva, se considerado que ele impõe um dever de proteção ao Estado contra eventuais agressões (do próprio Estado e de particulares) a esse direito e estabelece diretrizes para a atuação dos poderes Executivo, Legislativo e Judiciário e para as relações entre particulares.

Frisa-se que o conjunto dessa análise se encontra disposto em três capítulos, constituindo, no entanto, o primeiro deles numa abordagem da formação e da evolução do direito à proteção de dados pessoais enquanto direito fundamental no sistema jurídico da União Europeia. Isso porque o modelo europeu de regulamentação teve uma influência determinante na criação das regras e dos princípios relacionados ao tema no Brasil, como se verá adiante, contribuindo, ainda, para a internalização do direito à autodeterminação informativa, que hoje fundamenta a Lei nº 13.709/2018.

Assim, após o estudo da fundamentalidade material do direito à proteção de dados e da construção, ao mesmo tempo, da sua estrutura dogmática, no segundo capítulo, o terceiro e último capítulo propõe uma análise jurisprudencial do tema, verificando como foram os primeiros tratamentos dados pelos Tribunais à proteção de dados no Brasil, antes mesmo da edição da Lei nº 13.709/2018, e de que forma leis setoriais, como o Código de Defesa do Consumidor e a Lei do Marco Civil, por exemplo, ajudaram no amadurecimento da matéria e na definição da sua relevância.

Ato contínuo, esse trabalho apresenta a visão do Supremo Tribunal Federal, através das suas ainda tímidas e recentes decisões sobre proteção de dados, demonstrando, mais uma vez, a atualidade do tema, ao mesmo tempo em que analisa a decisão nos autos da ADI nº 6387

MC/DF, que representou um marco no sistema jurídico pátrio ao reconhecer, pela primeira vez, um direito fundamental à proteção de dados.

Dessa forma, a presente pesquisa, que se torna empírica por buscar respostas para uma problemática a partir de situações reais, utilizará o método de abordagem dedutivo, com a apresentação do tema na sua perspectiva teórica, partindo do estudo dos princípios gerais e regras específicas da Lei nº 13.709/2018, além de normas constitucionais para atingir o objetivo desejado, qual seja a análise da fundamentalidade material do direito à proteção de dados e da sua estrutura dogmática.

Por essa razão, trata-se, ainda, de pesquisa qualitativa e exploratória, posto que as doutrinas sobre a questão debatida ainda são incipientes, o que fez com que a autora desse trabalho se valesse de doutrinas e artigos científicos na área de Direito Constitucional para explorar o assunto e construir a presente análise, tendo as lições do jurista Ingo Wolfgang Sarlet contribuído sobremaneira para o desenvolvimento da base de hipóteses acerca da supracitada fundamentalidade material do direito à proteção de dados.

Buscou-se, dessa forma, uma compreensão inicial do tema, permitindo que pesquisas futuras desenvolvam e validem o estudo realizado nesta dissertação, que contou com contribuições também relevantes de doutrinadores especialistas na área, como Laura Schertel, Danilo Doneda, dentre outros, evidenciando o método bibliográfico utilizado, que ainda teve como fonte doutrinas e jurisprudências estrangeiras, principalmente europeias, tendo em vista a forte influência do direito europeu na construção das bases do direito à proteção de dados no Brasil, sendo inerente, portanto, o estudo do direito comparado nessa dissertação.

Essa autora pretende, assim, contribuir com a doutrina constitucional e especializada no tema, mas sem esgotar toda a sistemática da proteção de dados, dado o objetivo geral desse trabalho, que é analisar a matéria apenas sob o enfoque constitucional, visando a compreensão de suas múltiplas dimensões à luz da Constituição Federal, mas sem esquecer de reforçar a necessidade atual e constante do debate acerca da proteção de dados nesse novo cenário social e econômico, no qual o indivíduo ganha o papel de protagonista.

2 A FORMAÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

2.1 A REGULAMENTAÇÃO DO DIREITO À PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

O inevitável desenvolvimento tecnológico nas organizações sociais modernas foi responsável por tornar cada vez mais sutil os limites entre a esfera pública e a esfera privada, redefinindo o conceito de privacidade[8]. Esse fenômeno decorreu tanto do advento das tecnologias de informação e comunicação, a partir da década de 1950, como da popularização da *Internet*, fazendo com que se mostrasse insuficiente o modo tradicional de armazenamento de informações.

Conforme lembra Ruaro; Rodriguez e Finger (2011, p. 48):

> Na sociedade pré-industrial, a documentação acerca das relações pessoais era restrita a uma pequena parte da vida das pessoas, e isso ocorria dentro de uma elite reinante. A rotina diária das pessoas comuns não era documentada de forma escrita. Isto por ser extremamente fácil conseguir coletar, havendo necessidade, todos os tipos de dados possíveis destes cidadãos, tendo em vista que a maioria das relações pessoais se dava proximamente.

As informações passaram, então, a ser utilizadas das mais variadas formas e para um número indeterminado de finalidades graças ao desenvolvimento de potentes *softwares*, que permitem um registro massivo de dados relativos à vida privada de indivíduos. Esse grande volume de dados, gerados a todo momento, tornou possível o cruzamento de informações através de diversas formas e utilizadas para as mais variadas finalidades, levando a um aumento da capacidade qualitativa de processamento e transmissão dessas informações, mas também interferindo nas relações sociais.

Isso fez com que, ao longo dos anos, a informação passasse a ser o elemento nuclear para o desenvolvimento da economia, conforme lembra Bruno Bioni (2020, p.4), chamando a

[8] O tema da privacidade tem relação direta com o nível de desenvolvimento tecnológico da sociedade, abrangendo novas dimensões e elementos quando se trata da coleta e do tratamento de dados pessoais. Por isso, é importante ressaltar que ambos os termos não se confundem, tendo em vista que o núcleo da proteção dos dados pessoais é diferente do direito à privacidade. Aquele se volta para a proteção da pessoa, atraindo garantias mais amplas ao indivíduo do que as advindas da proteção da privacidade, podendo, por isso, ser alocado como um novo direito de personalidade, que exige instrumentos normativos exclusivos e individuais de proteção. Isso porque, conforme adverte Ana Frazão (2019, p.100), "os problemas que decorrem da exploração dos dados pessoais são muito mais extensos do que a mera violação da privacidade, especialmente se tal direito for compreendido sob a sua acepção clássica, ou seja, no sentido de intimidade e do direito de ser deixado só", o que coloca em risco até mesmo a autonomia e individualidade do cidadão. Por tais razões, esses direitos devem ser considerados autônomos, mesmo que estejam relacionados e se sobreponham em parte.

atenção tanto do setor privado quanto do setor público, que descobriram que importantes diretrizes sobre os hábitos de consumo dos cidadãos, além de outros dados pessoais, poderiam ser obtidos para a sua utilização na atividade empresarial e na Administração Pública, tornando a informação numa verdadeira fonte de geração de riquezas.

Assim, a emergência de um novo paradigma tecnológico organizado em torno de novas tecnologias da informação, mais flexíveis e poderosas, possibilitou que a própria informação se tornasse produto do processo produtivo[9] (CASTELLS, 2019, p. 135), passando a ser reconhecida como fenômeno relevante juridicamente (DONEDA, 2019, p. 138) e demandando uma proteção adequada em face de seus registros, distorções e manipulações (RUARO; RODRIGUEZ; FINGER, 2011, p. 50).

Conforme pontua Rodotà (2008, p. 63):

> A proteção de dados pessoais foi ganhando, dessa forma, autonomia própria e provocando o desenvolvimento paralelo de leis relacionadas ao tema, delineando uma nova fronteira despertada pela crescente consciência da necessidade de um enfoque global voltado para o tema.

No entanto, num primeiro momento, uma normatização específica sobre a proteção de dados teve como fundamento os interesses do Estado, no período pós-guerra, quando a máquina administrativa percebeu que as informações pessoais dos seus cidadãos eram úteis para planejar e coordenar as suas ações para um crescimento ordenado (BIONI, 2020, p. 109).

Exemplo disso ocorreu nos Estados Unidos, em 1965, com a criação do projeto *National Data Centers*, pensado com o objetivo de criar um banco de dados unificado sobre cidadãos norte-americanos para uso do Poder Público, no qual seria possível reunir, ao mesmo tempo, cadastros do Censo, registros trabalhistas, fiscais e relativos à Previdência Social, permitindo o controle e acompanhamento irrestrito de dados pessoais da população.

Para o governo americano, na época, a centralização das informações pessoais dos cidadãos num único registro seria uma natural evolução da estrutura administrativa diante dos avanços proporcionados pela informática. Entretanto, por suscitar acirradas discussões sobre a ameaça que esse projeto representaria para as liberdades individuais, ele nunca saiu do papel[10].

---

[9] Nesse sentido, Castells (2019, p. 176) ainda complementa afirmando que informação e conhecimento são elementos cruciais no crescimento da economia, sendo "a geração de conhecimentos e a capacidade tecnológica ferramentas fundamentais para a concorrência entre empresas, organizações de todos os tipos e, por fim, países".

[10] Conforme lembra Laura Schertel Mendes (2014, p.39), com esse projeto, que permitiria a formação de um único centro de dados nacional, os demais órgãos do governo eximir-se-iam de investir em informática e em tecnologias de armazenamento. Essa possibilidade culminou "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 dos cidadãos", fazendo com que a execução desse projeto fosse frustrada.

Tendo em vista, ainda, que propostas semelhantes de centralização de banco de dados foram feitas pelas Administrações Públicas de outros países[11], causando, tal qual ocorreu nos Estados Unidos, debates mais profundos a respeito da privacidade dos cidadãos, pode-se afirmar que a primeira geração de normas[12] de proteção de dados acabou consistindo numa reação às intenções de controle da Administração Pública sobre os dados pessoais dos indivíduos.

Dentre as primeiras legislações, destaca-se a Lei do *Land* alemão de Hesse, de 1970, a chamada *Hessisches Datenschutzgesetz*, que buscava regulamentar os bancos de dados governamentais e foi pioneira ao se preocupar com a coleta e tratamento de dados pessoais sem tratar do tema de forma objetiva, mas apenas de maneira genérica. Conforme lembra Danilo Doneda (2011, p. 96), "essas leis buscavam enfatizar o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas".

Além dela, citam-se também a primeira lei nacional de proteção de dados editada na Suécia, em 1973, conhecida como *Datalegen*[13], e a Lei Federal de Proteção de Dados da Alemanha, de 1977, que guardam como características comuns a todas as leis dessa primeira geração a tentativa de controlar a criação dos bancos de dados governamentais através da concessão de autorizações para o seu funcionamento, usando licença prévia, por exemplo[14].

Registra-se que, nesse primeiro momento, a estrutura de tais leis não contemplava a participação do cidadão nesse processo, trazendo normas específicas destinadas apenas aos agentes diretamente responsáveis pelo processamento de dados. Conforme lembra Doneda

---

[11] Ressalta-se que, em outros países, houve iniciativas governamentais semelhantes, provocando o mesmo debate público. Foi o que ocorreu, por exemplo, na Suécia, onde o Parlamento propôs, em 1960, a fusão de informações fiscais e civis com os dados do censo, e também na França, com o projeto SAFÁRI (Système Automatisé pour les *F*ichiers *A*dministratifs et le *R*épertoire des *I*ndividus), de 1970, que objetivava transferir os dados pessoais dos cidadãos franceses para a administração pública, formando um sistema único automatizado, através do qual cada cidadão passaria a ser identificado por um número por toda a sua vida. Tais projetos também não tiveram sucesso e foram encerrados, pelos mesmos motivos do projeto norte-americano. Entretanto, lembra Doneda (2019, p. 165), na França, esse debate influenciou o surgimento da lei francesa de proteção de dados pessoais, em 1978, conhecida como *Loi Informatique, Fichiers et Libertés*.

[12] Essa dissertação segue a classificação utilizada por Mayer-Schoneberger, que identifica quatro gerações de leis relacionadas à proteção de dados.

[13] Assim como a Lei de Hesse, a Lei Sueca de Dados de 1973 abrangeu apenas o processamento de dados pessoais em registros tradicionais e informatizados. O ato não continha muitas disposições materiais sobre quando e como os dados deveriam ser processados nem tratava de princípios norteadores para a proteção de dados. Mesmo assim, essa lei já trazia a previsão do tema como agenda pública governamental.

[14] Nesse ponto, destaca Mendes (2014b, p. 38) que "o impulso para o surgimento dessas normas foi o contexto generalizado do Estado Social, que requeria, para o funcionamento de sua burocracia, um planejamento sofisticado, o que, por sua vez, somente poderia ser alcançado por meio da coleta e do processamento dos dados dos cidadãos".

(2019, p. 176), elas até traziam em seu bojo princípios de proteção, mas muitas vezes abstratos e amplos, focalizados basicamente na atividade do processamento de dados.

Ocorre que, com a crescente evolução tecnológica e o aumento generalizado de centros de processamento de dados, ultrapassando os limites da seara pública e substituindo a ideia de um banco de dados único, tais legislações acabaram se tornando obsoletas, embora tenham servido como fonte dos principais e mais completos conjuntos de leis sobre o tema ao longo dos anos. De acordo com Danilo Doneda (2019, p. 176):

> Estas leis de proteção de dados de primeira geração não demoraram muito a se tornarem ultrapassadas, diante da multiplicação dos centros de processamento de dados, que tornou virtualmente difícil propor um controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento.

Isso decorreu do desenvolvimento das tecnologias de informação e da utilização cada vez mais significativa de dados pessoais por terceiros através de bancos conectados em rede, o que fez com que a problemática agora estivesse voltada para a privacidade dos cidadãos, exigindo que as técnicas de controle passassem a se preocupar mais com as liberdades negativas e a liberdade individual em geral, e não mais com procedimentos em si, dando lugar à segunda geração de normas de proteção de dados, mais preocupada com o indivíduo.

Como reflexo dessa nova mentalidade, destaca-se a edição da lei francesa de proteção de dados pessoais, de 1978[15], e as leis da Áustria, da França, da Dinamarca e da Noruega, tendo, inclusive, a ideia de privacidade informacional sido introduzida, pela primeira vez, em Constituições da época, como ocorreu nas Cartas da Espanha e de Portugal[16].

---

[15] O que mais chama a atenção na lei francesa de proteção de dados, de 1978, é a instituição da Comissão Nacional de Informática e Liberdades (CNIL), um órgão autônomo dentro da estrutura do Estado incubido de zelar pela transparência e fixação de regras deônticas no tratamento automatizado de informações pessoais, através de alguns princípios norteadores, tais como o dever de lealdade na coleta de dados, com a imposição de sanção em caso de coleta fraudulenta; o respeito à finalidade declarada, o qual determinava que o tratamento de dados deveria atender a uma finalidade específica, prevendo também a imposição de sanção nos casos de utilização para fins diversos do declarado; o dever de informação às pessoas, que impunha que as pessoas cujos dados fossem coletados deveriam ser informadas, sob pena de multa em caso de descumprimento; e o dever de proteção dos dados sensíveis, com o intuito de proteger os dados relativos à origem racial, opiniões políticas, filosóficas ou religiosas, bem como os dados referentes às preferências sexuais e outros ligados à intimidade das pessoas, sob pena de multa e prisão em caso de desobediência. Tais regras, pautadas nos princípios da Declaração dos Direitos do Homem e do Cidadão, acabaram servindo como fonte de inspiração para outros países, na confecção de suas leis específicas de proteção de dados que começaram a eclodir a partir das décadas seguintes.

[16] A Constituição de Portugal de 1976, na sua primeira redação, já previa o direito à intimidade da vida privada e familiar e proibia a utilização abusiva de informações relativas às pessoas e famílias, em seu art. 33. No art. 35, por sua vez, reconhecia ainda o direito dos cidadãos de tomar conhecimento dos dados constantes dos registos mecanográficos a seu respeito, bem como o direito de retificar e atualizar esses mesmos dados, impedindo o tratamento de dados referentes a convicções políticas, religiosas ou de vida privada. É o que se depreende da sua leitura, *in verbis:*

"1. Todos os cidadãos têm o direito de tomar conhecimento do que constar de registros mecanográficos a seu respeito e do fim a que se destinam as informações, podendo exigir a rectificação dos dados e a sua actualização.

Tais diplomas significaram, assim, uma mudança de paradigma, já que se percebeu que "o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social" (DONEDA, 2019, p. 177), sendo as leis da segunda geração sobre esse tema fruto dos crescentes debates sobre consentimento bem como sobre o direito de acesso às próprias informações e a transparência em relação à existência dos bancos de dados de informações pessoais e dos seus critérios básicos de funcionamento (DONEDA, 2010).

Nesse contexto, o objeto do direito à privacidade amplia-se, como efeito do enriquecimento da noção técnica da esfera privada, a qual compreende um número sempre crescente de situações juridicamente relevantes. Assim, já nesse período, "a extensão da área abrangida pela tutela da privacidade fez com que aumentasse, paralelamente, o número de sujeitos interessados em tal proteção bem como sua relevância social" (RODOTÀ, 2008, p. 93).

Depreende-se, portanto, que a mudança no tratamento da matéria, com a colocação do indivíduo como protagonista na proteção dos seus dados e com o reconhecimento da privacidade como um direito fundamental em algumas Constituições, ilustra bem a importância dada pelos países europeus ao tema, tornando esse continente fonte dos principais e mais completos conjuntos de leis sobre proteção de dados pessoais que passaram a eclodir ao longo das décadas seguintes[17].

E foi exatamente essa autonomia dada ao indivíduo para controlar o fluxo das suas informações pessoais que marcou a passagem para a terceira geração de leis de proteção de dados, quando surgiu então o denominado direito à autodeterminação informativa.

2.2 O DIREITO À AUTODETERMINAÇÃO INFORMATIVA

A ideia de autodeterminação informativa coincide com a denominada terceira geração de leis de proteção de dados pessoais, que se destaca com decisão da Corte Constitucional Alemã, datada de 15 de dezembro de 1983, que declarou parcialmente inconstitucional uma lei

2. A informática não pode ser usada para tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se trate do processamento de dados não identificáveis para fins estatísticos. 3. É proibida a atribuição de um número nacional único aos cidadãos" (PORTUGAL, 1976).

[17] É importante frisar que o modelo europeu de proteção de dados difere-se do modelo americano no sentido de que, enquanto este se estruturou a partir da ideia do *right to privacy* (privacidade), desenvolvendo-se originalmente na jurisprudência e doutrina norte-americanas, aquele é mais sistemático, desenvolvendo-se a partir de regulações elaboradas em nível de direito comunitário, com a adoção de soluções pontuais para o problema da proteção de dados. O modelo europeu estruturou-se a partir de uma Diretiva, instrumento normativo típico da União Europeia, como se verá adiante.

que disciplinava o censo populacional, conhecida como Lei do Censo Alemã (*Volkszählungsurteil*).

Essa lei tinha como finalidade realizar censo estatístico através da coleta de dados pessoais através de perguntas de cunho pessoal, como nome, endereço, convicções religiosas, dentre outras, que seriam posteriormente submetidas a tratamento informatizado, com o cruzamento de outros registros públicos. Além disso, previa o compartilhamento desses dados da população com repartições públicas para fins de execução de atividades administrativas, prevendo até uma multa em caso de recusa daqueles que se recusassem a responder tais perguntas, conforme se depreende dos seguintes dispositivos, *in verbis*:

> § 10
> (1) Todas as pessoas físicas e jurídicas sob o direito privado, bem como parcerias e órgãos, instituições e fundações sob o direito público, autoridades e outros órgãos públicos da Confederação, o Länder, municípios e associações municipais e seus órgãos, instituições e fundações sob o direito público são obrigados a responder às perguntas devidamente organizadas, a menos que a resposta seja expressamente independente.
> (2) Os respondentes são obrigados a fornecer informações em relação aos órgãos e pessoas oficialmente encarregadas da implementação das estatísticas federais.
> 3. A resposta será dada com sinceridade, na íntegra, a tempo e gratuitamente e postagem.
> 4. Quando forem fornecidos formulários de pesquisa para a conclusão do entrevistado, as respostas aos formulários de pesquisa serão fornecidas. A exatidão das informações deve ser confirmada por assinatura, na medida em que prevista no formulário de pesquisa (ALEMANHA, 1983, tradução nossa).

A Lei do Censo acabou tendo uma repercussão negativa em razão do sentimento de insegurança que se gerou entre a população alemã, levando o Tribunal Constitucional alemão a declarar a sua inconstitucionalidade parcial, por entender que "estaria caracterizada a diversidade de finalidades, o que impediria que o cidadão conhecesse o uso efetivo que seria feito de suas informações" (DONEDA, 2019).

Ainda de acordo com essa decisão,

> Não seria compatível com a dignidade humana se o Estado pudesse se arrogar ao direito de registrar e catalogar o cidadão coercitivamente, atingindo toda a sua personalidade, mesmo dentro do sigilo de uma pesquisa estatística, e tratá-lo, em todos os aspectos, como uma coisa suscetível de ser inventariada" (MARTINS, 2005, p. 217).

Com isso, pela primeira vez, a proteção de dados passou a ser vista como um direito de personalidade autônomo[18], a partir da ideia de uma autodeterminação informativa que conferia

[18] Afirmam Hornung e Schnabel (2009, p. 84) que "[...] no entendimento alemão, o direito à autodeterminação informacional, como o âncora constitucional para a proteção de dados, é uma parte do direito geral da

ao indivíduo o poder de decidir se e em que medida poderia divulgar aspectos de sua vida pessoal.

Dessa forma, a coleta de dados prevista pela Lei do Censo de 1983 não poderia catalogar a personalidade de uma pessoa de maneira incompatível com a dignidade humana, só cabendo a coleta e uso dos dados pessoais para fins estatísticos[19]. Além disso, o Tribunal Constitucional alemão reconheceu ainda que o cidadão fosse informado previamente sobre a coleta e processamento dos seus dados, atendendo, assim, ao princípio da finalidade, conforme se depreende do seguinte trecho:

> A lei está em conflito com a exigência de materialidade estabelecida pelo Tribunal Constitucional Federal pelo seu silêncio sobre certas questões importantes de sua aplicação. O objetivo da pesquisa e do programa de pesquisa deve ser regulado por lei. No entanto, a Lei Censitária regulamenta o processo de contagem em si apenas com uma sentença insignificante, deixando em aberto, assim, a forma de medidas que afetam os direitos fundamentais. Além disso, é constitucionalmente necessário que o cidadão seja informado sobre o processamento, em especial a transferência de seus dados; caso contrário, o sigilo estatístico não seria suficientemente protegido pelo crime do nº 203 do StGB, que foi concebido como crime (TCF, on-line, tradução nossa).

De todo modo, foi mantida a realização do censo na Alemanha; no entanto, por determinação do referido Tribunal, foram assegurados meios que resguardassem a segurança dos dados dos cidadãos que seriam entrevistados bem como proibidas a transferência de alguns tipos de dados, como nome e endereço, a outros órgãos de governo.

A autodeterminação informativa surgia, assim, como um direito fundamental, reflexo da crescente preocupação com os avanços tecnológicos da época, conforme lembra Rodotà (2008, p. 96):

> A presença de riscos conexos ao uso das informações coletadas, e não uma natural vocação ao sigilo de certos dados pessoais, foi o que levou ao reconhecimento de um "direito à autodeterminação informativa" como direito fundamental do cidadão. Este reconhecimento enquadra-se na tendência de atribuir a condição de direitos fundamentais a uma série de posições individuais e coletivas relevantes no âmbito da informação.

---

personalidade. Isto é, portanto, intimamente ligado e serve a ideia de dar a cada pessoa a possibilidade de desenvolver uma personalidade livre e autodeterminada. Com base nisso, o direito à autodeterminação informacional sempre foi restrito às pessoas físicas e não pode ser invocado por pessoas jurídicas entidades".

[19] É o que se depreende do seguinte trecho da sentença do Tribunal Constitucional alemão: "Se os indivíduos não puderem, com certeza suficiente, determinar que tipo de informação pessoal é conhecida em seu ambiente, e se for difícil determinar que tipo de informação os potenciais parceiros de comunicação têm acesso, isso pode prejudicar seriamente a liberdade de exercer autodeterminação. No contexto do moderno processamento de dados, o livre desenvolvimento da personalidade de alguém exige, portanto, que o indivíduo seja protegido contra a coleta, armazenamento, uso e compartilhamento ilimitados de dados pessoais.

Por consequência, houve uma transformação do poder social, consubstanciada na ideia de que, a partir de então, o cidadão adquiria o poder de determinar e controlar a utilização de seus dados pessoais, através do consentimento, que acabou se tornando um parâmetro para as leis de proteção de dados que surgiram posteriormente[20], como aquelas que marcaram a quarta geração de normas.

Segundo Rodotá (2008, p. 148),

> Os elementos-chave desse modelo, portanto, são o consentimento do interessado e o seu direito de acesso a todas as coletâneas de informações. Trata-se de um poder difuso, que não requer mediações burocráticas, visto que o acesso é exercido diretamente pelo interessado frente a todos os sujeitos, públicos e privados, que recolhem dados pessoais.

Assim, esse novo sistema jurídico, do qual faz parte a quarta geração de normas de proteção de dados, passou a ser calcado em princípios fundamentais de proteção, cuja aplicação se torna "a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos" (DONEDA, 2011, p. 101).

Dentre tais princípios, destaca-se o da finalidade, que comanda que o tratamento de dados seja feito para uma finalidade específica, devendo o detentor dos dados tomar conhecimento sobre a finalidade da coleta e utilização dos seus dados, bem como os princípios da publicidade, da exatidão, do livre acesso e da segurança física e lógica[21], que também surgiram com o objetivo de fortalecer a posição dos indivíduos e reconhecer o desequilíbrio nessa relação[22].

---

[20] Nesse sentido, Mendes (2014b, p. 42) lembra que "a principal diferença dessa fase em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre "tudo ou nada"". Segundo a autora, são exemplos dessa terceira geração de normas a emenda à Lei Federal de Proteção de Dados alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e previsão constitucional da proteção de dados pessoais da Holanda.

[21] Doneda (2011), faz uma síntese de tais princípios: *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos; *Princípio da exatidão*: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade; *Princípio do livre acesso*, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos; *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado (grifo nosso).

[22] Ainda segundo Doneda (2011), "estes princípios, mesmo que fracionados, condensados ou adaptados, formam a espinha dorsal das diversas leis, tratados, convenções ou acordos entre privados em matéria de proteção de dados

Chama atenção também a previsão em tais leis da existência de autoridades independentes para tutela desses dados, a fim de tornarem efetivos os direitos dos cidadãos, bem como o surgimento de normas que retiraram da esfera do controle do indivíduo o papel da decisão individual de autodeterminação informativa. Segundo Doneda (2019, p. 179), "isto ocorre porque se parte do pressuposto de que determinadas modalidades de tratamento de dados pessoais necessitam de uma proteção no seu mais alto grau, à qual não pode ser conferida exclusivamente a uma decisão individual"[23].

Diante disso, é possível observar que a decisão do Tribunal Constitucional alemão consistiu em verdadeiro marco da proteção de dados, estabelecendo diretrizes que influenciaram legislações, doutrinas e jurisprudências de diversos países relacionadas à autodeterminação informativa, fomentando a discussão no âmbito constitucional sobre o tema, ao exigir que a sua limitação ou restrição adquirisse base jurídica constitucional.

Com a decisão alemã, a proteção de dados se estabelece, ainda, como uma evolução do direito à privacidade, configurando-se como uma extensão da própria personalidade do indivíduo, capaz de identificá-lo em suas singularidades, cuja violação põe em risco a sua autonomia como ser social.

2.3 O MODELO EUROPEU DE PROTEÇÃO DE DADOS

O reconhecimento da autodeterminação informativa foi o ponto de partida para a multiplicação de diversos instrumentos jurídicos que objetivavam a proteção de dados, exprimindo o direito europeu muito bem esse desenvolvimento quantitativo e qualitativo das normas protetivas relacionadas aos dados pessoais.

A preocupação com o surgimento de novas tecnologias aliada a dificuldade cada vez maior de controle na coleta e uso desses dados, levou à necessidade de uma uniformização legislativa supranacional e de criação de ações coordenadas voltadas para a aplicação e fiscalização das leis voltadas para o tema.

---

pessoais, formando o núcleo das questões com as quais o ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais".

[23] A respeito de tais normas, Simitis (2012 apud MENDES, 2014b, p. 43) lembra que isso "pode ser observado na proibição, total ou parcial, imposta para o tratamento de dados considerados sensíveis, que são aqueles cujo tratamento tem grande potencial de acarretar discriminação, tais como os dados relativos à etnia, opção sexual, opinião política e religião.

Nesse contexto, surgem as *guidelines* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[24], dentre as quais se destacam as *Guidelines on the Prtotection of Privacy* e *Transborder Flows of Personal Data*, que foram revisadas em 2013 e influenciaram o desenvolvimento da proteção de dados ao recomendar um padrão normativo através de princípios que deveriam nortear essa atividade de regulação. A ideia, segundo Bruno Bioni (2020, p. 114) "[...] era criar um ambiente regulatório uniforme entre os países-membros e, ante a inexistência de disparidades regulatórias, garantir o livre trânsito das informações"[25].

Esse movimento provocado pela OCDE influenciou, posteriormente, o Conselho da Europa a realizar a Convenção de Strasbourg, em 1981, conhecida também por Convenção 108, que teve como função, de acordo com Doneda (2019, p. 194), incitar "[...] os estados-membros do Conselho da Europa e demais signatários da Convenção a adotar normas específicas para o tratamento de dados pessoais, consonantes aos seus próprios parâmetros de proteção".

Essa convenção, ratificada por todos os países membros do Conselho da Europa, foi o primeiro instrumento internacional juridicamente vinculativo no âmbito da proteção de dados, tornando-se uma referência no modelo europeu por tratar o tema como assunto de direitos humanos[26], fazendo com que vários países europeus adequassem suas legislações de acordo com suas normas[27].

Conforme lembra Bennett (2018, p.240):

> Progressivamente, esses esforços de harmonização padronizaram o que significava para um país para buscar proteção de dados adequada, e para organizações para processar dados pessoais de forma responsável. À medida que mais países aderiam ao "clube" de proteção de dados, aumentava a pressão sobre aqueles fora do clube para aprovar leis equivalentes.

---

[24] A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) é uma organização internacional criada em 1961 com o objetivo de promover o desenvolvimento econômico e estimular o comércio mundial. É formada atualmente por 37 países membros e através das *guidelines* estabelece recomendações dirigidas para empresas multinacionais que operam nos países aderentes, fornecendo princípios e padrões não vinculativos para uma conduta comercial responsável. Disponível em: http://mneguidelines.oecd.org/guidelines/. Acesso em 09 set. 2020.

[25] Nesse aspecto, Doneda (2019, p. 193) reforça que a preocupação central das *guidelines* "era com o tráfego de dados e não com a sua proteção em si". No entanto, tais documentos já traziam em seu bojo referenciais que seriam utilizados em legislações posteriores, como conceito de dados pessoais, princípios norteadores e o papel do consentimento do titular dos dados.

[26] Logo no artigo 1º da Convenção 108, essa norma deixa clara a garantia desse direito: "A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»)". Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId =0900001680078b37. Acesso em 10 set. 2020.

[27] Ressalta-se que, como a Convenção 108 tem um caráter aberto à adesão de Estados que não pertençam ao Conselho da Europa, países não integrantes desse Conselho também ratificaram esse instrumento normativo. Em 2018, o Brasil aderiu ao Comitê Consultivo como observador.

Esse processo de convergência de políticas com a intenção de criar um modelo comum europeu de proteção de dados levou, em 1995, à edição da Diretiva 95/46/CE[28] pelo Parlamento Europeu e pelo Conselho da União Europeia, cujo teor trata da proteção de dados singulares quanto ao tratamento e à livre circulação destes dados e buscou concretizar as finalidades propostas pela Convenção 108, no sentido de impor aos estados-membros do Conselho que harmonizassem suas leis conforme o conteúdo dessa Diretiva[29].

Merece destaque, nessa Diretiva, a menção ao termo direitos fundamentais em suas considerações iniciais[30], denotando desde já a sua preocupação com a proteção da pessoa ao mesmo tempo em que assegura a livre circulação de dados de um Estado-membro para outro, desdobrando-se seu objetivo em dois eixos, conforme explica Doneda (2019, p. 198):

> Verificamos, portanto, a presença dos dois eixos em torno dos quais a disciplina se estrutura – a proteção da pessoa e a necessidade de proporcionar a livre circulação de "pessoas, mercadorias, serviços e capitais" no espaço comunitário, o que implica a circulação de dados pessoais – bem como a presença de um critério de equilíbrio entre ambos, que é a referência ao homem e aos seus direitos fundamentais, reconhecida como base e fundamento de toda a disciplina.

[28] As diretivas europeias desempenham um importante papel integrador no direito comunitário, à medida que se tratam de instrumentos normativos que fixam objetivos a serem atingidos pelos Estados-Membros. Uma vez adotada a nível da União Europeia, a diretiva é incorporada ou transposta pelos países, passando a vigorar como lei nesses locais.

[29] Por essa razão, é possível afirmar que a Diretiva 95/46/CE constituiu na base de desenvolvimento das legislações nacionais de cada Estado-membro. Fica clara essa determinação nas considerações desse documento: (21) Considerando que a presente directiva não prejudica as regras de territorialidade aplicáveis em matéria de direito penal; (22) Considerando que os Estados-membros precisarão, na sua legislação ou nas regras de execução adoptadas nos termos das presente directiva, as condições gerais em que o tratamento de dados é lícito; que, nomeadamente, o artigo 5º, conjugado com os artigos 7º e 8º, permite que os Estados-membros estabeleçam, independentemente das regras gerais, condições especiais para o tratamento de dados em sectores específicos e para as diferentes categorias de dados referidas no artigo 8º. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT> Acesso em 10 set. 2020.

[30] Convém expor as três considerações iniciais dessa Diretiva: (1) Considerando que os objectivos da Comunidade, enunciados no Tratado, com a redacção que lhe foi dada pelo Tratado da União Europeia, consistem em estabelecer uma união cada vez mais estreita entre os povos europeus, em fomentar relações mais próximas entre os Estados que pertencem à Comunidade, em assegurar o progresso económico e social mediante acções comuns para eliminar as barreiras que dividem a Europa, em promover a melhoria constante das condições de vida dos seus povos, em preservar e consolidar a paz e a liberdade e em promover a democracia com base nos direitos fundamentais reconhecidos nas Constituições e leis dos Estados-membros, bem como na Convenção europeia para a protecção dos direitos do Homem e das liberdades fundamentais. (2) Considerando que os sistemas de tratamento de dados estão ao serviço do Homem; que devem respeitar as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada, e contribuir para o progresso económico e social, o desenvolvimento do comércio e o bem-estar dos indivíduos; (3) Considerando que o estabelecimento e o funcionamento do mercado interno no qual, nos termos do artigo 7º A do Tratado, é assegurada a livre circulação das mercadorias, das pessoas, dos serviços e dos capitais, exigem não só que os dados pessoais possam circular livremente de um Estado-membro para outro, mas igualmente, que sejam protegidos os direitos fundamentais das pessoas. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT> Acesso em 10 set. 2020.

A Diretiva 46/95/CE ainda incluiu em seu bojo aspectos importantes relacionados à atividade de processamento de informações, tais como o conceito de dados pessoais, a previsão de tratamento de dados pessoais, que pode se dar com ou sem meios automatizados, a função do responsável pelo tratamento, o conceito de destinatário dos dados bem como a possibilidade de consentimento do titular, assegurando ao indivíduo o controle sobre as suas informações pessoais.

E por exigir que cada Estado-membro previsse uma agência ou comissário de proteção de dados, pode-se afirmar, conforme lembra Bioni (2020, p. 118) que a Diretiva 46/95/CE trouxe "[...] uma abordagem regulatória que se centra nesses dois atores – o titular das informações pessoais e quem as processa – para, por meio de direitos e obrigações simétricas, ser garantido o prometido controle dos dados pessoais".

Em 2002, foi editada a Diretiva 2002/58/CE sobre o tratamento e a proteção da privacidade nas comunicações eletrônicas[31], que não inovou o modelo já produzido pela Diretiva 46/95/CE, mas trouxe especial menção à Carta dos Direitos Fundamentais da União Europeia[32], proclamada em 7 de dezembro de 2000, que, por sua vez, trouxe em seu art. 8º a previsão do direito à proteção de dados, distinguindo-o, pela primeira vez, do direito ao respeito pela vida privada e familiar presente no art. 7º, projetando claramente o direito à proteção de dados pessoais na esfera de direitos fundamentais.

Afirma o art. 8º da Carta dos Direitos Fundamentais da União Europeia, *in verbis*:

> 1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente (PARLAMENTO EUROPEU, 2000).

[31] Regulando apenas o tratamento de dados pessoais e a proteção da privacidade no âmbito das prestações de serviços de comunicações eletrônicas acessíveis ao público em redes de comunicações públicas, essa Diretiva aborda questões específicas e sensíveis como a conservação de dados de conexão para fins de faturamento dos serviços de conexão prestados, o envio de mensagens eletrônicas não solicitadas (spam), a utilização de dados pessoais em listagens públicas (como listas telefônicas), e a utilização dos chamados "testemunhos de conexão" ou cookies (GUIDI, 2019).

[32] É o que se depreende das considerações iniciais dessa Diretiva: "(2) A presente directiva visa assegurar o respeito dos direitos fundamentais e a observância dos princípios reconhecidos, em especial, pela Carta dos Direitos Fundamentais da União Europeia. Visa, em especial, assegurar o pleno respeito pelos direitos consignados nos artigos 7.o e 8.o da citada carta". Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32002L0058&from=PT> Acesso em 10 set. 2020.

Essa Carta, que traz disposições sobre direitos humanos e teve como objetivo dar maior visibilidade à proteção dos direitos fundamentais dos cidadãos europeus, reconheceu, assim, a proteção de dados como um direito individual, que se apresentou, na visão de Rodotá (2008, p. 184), como um direito "novo" e "autônomo", distinto da acepção tradicional de privacidade, contribuindo de forma decisiva para a "constitucionalização da pessoa"[33].

E mesmo com um sistema já consolidado de normas, o modelo europeu de proteção de dados sofreu grande alteração em 2016, quando foi introduzido o Regulamento nº 679/2016, que substituiu a Diretiva nº 95/46/CE e ficou conhecido internacionalmente como *General Data Protection Regulation* (GDPR) ou Regulamento Geral sobre a Proteção de Dados.

Conforme lembra Guilherme Guidi (2019, p. 421), "a substituição de uma diretiva por um regulamento veio atender a uma necessidade de unificação do sistema, já que, através do regulamento, não seria mais necessária a incorporação do texto supranacional por uma lei interna", como ocorria com a diretiva, o que torna o regulamento diretamente aplicável pelos países europeus. Além disso, ressalta Bennett (2018, p. 240):

> Havia também um desejo urgente de "modernizar" o sistema europeu de proteção de dados a fim de torná-lo relevante para a economia digital em rede global, na qual os serviços de redes sociais estavam gerando grandes volumes de conteúdo gerado pelo usuário, e os serviços de computação em nuvem estavam tornando as fronteiras geográficas cada vez mais irrelevantes.

O Regulamento Geral sobre a Proteção de Dados entrou em vigor em toda a União Europeia em 25 de maio de 2018, sendo um reflexo do crescente processo global de convergências políticas e comerciais que elevaram os padrões internacionais de privacidade, segundo Bennett (2018, p. 244), para quem "a adesão aos padrões de privacidade é agora considerada uma condição necessária para participação na economia internacional em rede"[34].

O GDPR, na verdade, revisou a Diretiva nº 95/46/CE, mas também estabeleceu novos princípios, padrões e regras para o tratamento de dados pessoais, além de aumentar as penalidades em razão da não conformidade pelas organizações, tendo exercido forte influência na Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil em agosto de 2020.

---

[33] A Carta dos Direitos Fundamentais da União Europeia se mostrou inovadora, ainda, em muitos sentidos, principalmente por incluir, dentre outros aspectos, a deficiência, a religião, a opinião política, as características genéticas, a diversidade cultural e linguística bem como a orientação sexual a salvo de qualquer discriminação, além de inserir a proteção de dados dentre os direitos fundamentais e prever a possibilidade de fiscalização do seu tratamento e acesso por parte de uma autoridade independente.

[34] Nesse sentido, Doneda (2019, p. 189) também lembra que "outra justificativa de peso foi a necessidade de atualização da disciplina de proteção de dados em diversos pontos, por conta do desenvolvimento dos sistemas de tratamento de dados pessoais e a sua integração com dinâmicas como a do Mercado Comum Digital".

Guidi (2019, p. 422) ainda complementa:

> Entre as principais alterações trazidas pelo GDPR, pode-se apontar algumas que são mais relevantes e que podem ser divididas por sua finalidade: alterações para reforçar os direitos dos usuários, alterações para reforçar as competências das Autoridades de Proteção de Dados, e alterações para *induzir e incentivar* certos comportamentos por parte dos responsáveis pelo tratamento" (grifo do autor).

Observa-se, dessa forma, que o modelo europeu de proteção de dados encontra-se atualmente na quarta geração de leis relativa a esse tema e, com o GDPR, ele inaugurou uma nova fase em seus esforços para a tutela dos dados pessoais, na qual o papel do consentimento ou a autodeterminação informativa permanecem como pré-requisitos para a coleta e tratamento de dados. Assim, segundo Rodotá (2008, p. 148), "[...] os elementos-chave desse modelo são, portanto, o consentimento do interessado e o seu direito de acesso a todas as coletâneas de informações".

Esse autor enfatiza também que:

> O modelo de tutela europeu nasceu do encontro da tradição americana de defesa da privacidade com a tradição europeia de tutela legislativa dos direitos do homem. Está fundamentado no reconhecimento de novos direitos fundamentais da pessoa e na criação de novas instituições de garantia (RODOTÁ, 2008, p. 149).

Mostra-se, assim, evidente, a partir da análise feita no presente capítulo, que o direito à proteção de dados acabou se tornando uma condição para a própria participação na vida pública, haja vista a importância dada à matéria e devido a sua projeção à categoria de direitos fundamentais por diversos países que adotaram esse modelo de proteção em seus ordenamentos[35], representando a proteção de dados uma verdadeira tutela da dimensão relacional da pessoa humana.

[35] Segundo Pinheiro (2020, p. 18), o Regulamento Geral sobre a Proteção de Dados ocasionou ainda um "efeito dominó", visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a União Europeia também deveriam ter uma legislação do mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da União Europeia.

3 O RECONHECIMENTO DA PROTEÇÃO DE DADOS COMO UM DIREITO FUNDAMENTAL NO BRASIL

O panorama legislativo atual brasileiro mostra-se bastante influenciado pelo sistema europeu de proteção de dados pessoais, aproximando-se deste na sua carga idealista e principiológica, com normas que, em sua maioria das vezes, apresentam condutas desejáveis e obrigatórias, mas que transferem aos aplicadores do Direito a definição dos padrões interpretativos que seriam razoáveis à manifestação do dever-ser[36].

Além do papel de destaque ocupado pelo consentimento na Lei Geral de Proteção de Dados, tal como ocorre no Regulamento Geral sobre a Proteção de Dados (RGPD), é possível observar ainda na legislação brasileira a elevação do direito à proteção de dados a uma categoria autônoma de direitos, desvencilhado da ideia de privacidade e vinculado à proteção da própria personalidade do indivíduo[37].

É o que se depreende da leitura do artigo 1º da Lei 13.709/2018 (LGPD) *in verbis*:

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

Esse entendimento, inicialmente desenvolvido pelo Tribunal Constitucional Federal alemão – na sentença que declarou a inconstitucionalidade parcial da Lei do Censo em 1983[38] – e adotado ao longo do histórico evolutivo de leis de proteção de dados na Europa, traz a ideia

---

[36] Kelsen (1998, p. 4), ao construir uma teoria pura do Direito, diferenciava o mundo do *ser*, próprio das ciências naturais, do *dever-ser*, no qual o Direito estava situado. De acordo com esse filósofo, o Direito "[...] é uma ordem normativa da conduta humana, ou seja, um sistema de normas que regulam o comportamento humano". Afirma ainda que o termo "norma" significa que algo deve ser ou acontecer, especialmente que um homem se deve conduzir de determinada maneira. É este o sentido que possuem determinados atos humanos que intencionalmente se dirigem à conduta de outrem".

[37] Conforme ensina Bioni (2020, p. 56-96), isso ocorre em razão da própria dinâmica da proteção dos dados pessoais, que foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Segundo esse autor, uma vez que, "[...] cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas e que hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses *signos identificadores* do cidadão, há uma série de liberdades individuais, atreladas ao direito à proteção de dados, que não são abraçadas pelo direito à privacidade".

[38] Nesse sentido, convém destacar o seguinte trecho da sentença da Corte alemã: "O direito geral da personalidade abarca, a partir da noção de autodeterminação, o poder conferido ao indivíduo para, em princípio, decidir se e em que medida divulgará aspectos de sua vida pessoal. Se os indivíduos não puderem, com certeza suficiente, determinar que tipo de informação pessoal é conhecida em seu ambiente, e se for difícil determinar que tipo de informação os potenciais parceiros de comunicação têm acesso, isso pode prejudicar seriamente a liberdade de exercer autodeterminação. No contexto do moderno processamento de dados, o livre desenvolvimento da personalidade de alguém exige, portanto, que o indivíduo seja protegido contra a coleta, armazenamento, uso e compartilhamento ilimitados de dados pessoais" (TCF, on-line, 1983, tradução nossa).

de que os dados pessoais são uma extensão da personalidade, constituindo, nas palavras de Costa e Oliveira (2019, p. 11), "[...] elementos substanciais de nossa singularidade, podendo ser compreendidos como reflexos pessoais capazes de nos identificar em nossas particularidades e enquanto seres sociais".

Isso porque é perfeitamente possível que, a partir de informações triviais coletadas de plataformas digitais, sejam revelados atributos da personalidade de um indivíduo, como orientação sexual, religiosa, política, racial, dentre outros dados sensíveis[39] passíveis de serem obtidos para a elaboração de perfis individuais e coletivos que podem levar a práticas discriminatórias com o uso inadequado desses dados pessoais[40]. Assim, as violações que podem ocorrer em um contexto de controle irregular e ilegal de dados pessoais alcançam muitas outras esferas do cidadão, colocando em risco até mesmo sua autonomia e individualidade (FRAZÃO, 2019, p. 100).

Por essa razão, afirma Mendes (2019, p. 124) que:

> A importância da tutela jurídica dos dados pessoais reside no fato de que esses dados, assim como as demais informações extraídas a partir deles, podem se constituir em uma representação virtual da pessoa perante a sociedade.
> […]
> A natureza do bem protegido, a própria personalidade a que os dados pessoais se referem, exige que a proteção de dados pessoais seja compreendida não como um direito à propriedade, mas como uma espécie dos direitos da personalidade.

Dessa forma, por se tratar de uma tutela da personalidade do indivíduo, a qual se relaciona ainda com outras liberdades e garantias fundamentais, fala-se na projeção da proteção de dados à categoria de direitos fundamentais, a exemplo do que já ocorre em outros países, como a Alemanha, que primeiramente reconheceu o direito à autodeterminação informativa no julgamento da já citada Lei do Censo, inserindo-o no rol de direitos fundamentais, bem como

[39] De acordo com a LGPD, dado pessoal sensível pode consistir em qualquer informação relacionada a uma pessoa física, identificada ou identificável, que trate sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político. Também podem ser considerados dados sensíveis aqueles referentes à saúde ou à vida sexual e dado genético ou biométrico da pessoa natural.

[40] Lembra Bioni (2020, p. 2014): "Coletam-se, cada vez mais, informações sobre um indivíduo, a fim de compor um perfil detalhado para alimentar análises preditivas a seu respeito. Isso equivale a classificá-lo e, até mesmo, segregá-lo. Da análise de crédito, do prémio fixado na apólice de seguro ao anúncio publicitário na rede social, tais práticas estão se tornando corriqueiras, parametrizando as oportunidades de nossas vidas".

Portugal[41], Espanha[42], além de outras nações[43], que, mesmo de forma implícita, consideram a proteção de dados como tal.

Frise-se que esses Estados acabaram por incorporar ao seu direito interno diversos aspectos da antiga Diretiva 95/46/CE, hoje substituída pelo Regulamento Geral sobre a Proteção de Dados (RGPD), que já seguia essa tendência em sua redação[44], o que revela a influência do modelo europeu de proteção de dados nos regramentos sobre o tema ao redor do mundo, não se podendo olvidar a importância da Carta de Direitos Fundamentais da União Europeia nesse contexto, que prevê, claramente, em seu artigo 8º, a proteção de dados enquanto direito fundamental[45].

No caso do Brasil, apesar de não existir, atualmente, previsão expressa de um direito fundamental autônomo à proteção de dados pessoais na Constituição Federal de 1988, já é possível verificar diversos entendimentos nesse sentido[46], a partir de uma interpretação sistemática da nossa Carta, que busca enquadrar a tutela dos dados no âmbito de proteção do artigo 5º, especificamente em seu inciso X, que trata da inviolabilidade da intimidade e da vida privada, e no inciso XII, que garante o direito ao sigilo de comunicações e dados.

---

[41] A Constituição portuguesa traz as seguintes disposições, em seu artigo 35, que trata da 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" (PORTUGAL, 2005).

[42] Por seu turno, a Constituição espanhola, em seu artigo 18.4, afirma: "A lei limitará o uso da informática para garantir a honra e a intimidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos" (ESPANHA, 1992), de onde se pode extrair a referência à proteção de dados como um direito fundamental garantido por essa Carta.

[43] Registra-se que o Chile, em 2018, através da Lei 21.096, consagrou em nível constitucional o direito à proteção de dados, acrescentando o número 4 ao artigo 19, que passou a ter a seguinte redação: 4º. "El respeto y protección a la vida privada y a la honra de la persona y su familia, 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". (CHILE, 2018) O mesmo ocorreu com México e Colômbia, que também já internalizaram o direito à proteção de dados em suas cartas constitucionais.

[44] Enquanto a redação da Diretiva 95/46/CE trazia, no decorrer do seu texto, a menção ao termo direitos fundamentais, sem correlacioná-lo, no entanto, diretamente à proteção de dados, o Regulamento Geral sobre a Proteção de Dados (RGPD) buscou ser mais direto, ao prever, logo em suas primeiras linhas, que "[...] a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental". (PARLAMENTO EUROPEU, 2016)

[45] Nesse ponto, Rodotá (2008, p. 236) ainda nos lembra que na, Carta de Direitos Fundamentais da União Europeia, o direito à proteção de dados está inserido no capítulo que se refere às liberdades. Segundo esse autor, a associação entre a privacidade e liberdade torna-se cada vez mais forte no momento atual europeu, tendo em vista que a tutela de diversas espécies de dados se torna uma premissa para o exercício das liberdades de expressão, de comunicação, de associação e de culto.

[46] No capítulo seguinte, será possível verificar o reconhecimento do direito à proteção de dados como um direito fundamental no âmbito jurisprudencial, especialmente na decisão recentemente proferida pelo Supremo Tribunal Federal, nos autos da ADI 6387 MC-Ref/DF, em 07.05.20, que serviu de paradigma nessa matéria.

Além disso, extrai-se indiretamente do teor do inciso LXXII o *status* de direito fundamental à proteção de dados, haja vista a possibilidade de conhecimento e retificação de dados através do *habeas data*[47], a despeito das limitações de ordem formal desse remédio constitucional.

Nesse sentido, convém expor a lição de Mendes (2014b, p. 168):

> Entendemos que é possível, a partir de uma interpretação sistemática da Constituição, fundamentar uma garantia geral de proteção de dados pessoais no sistema de direitos fundamentais: partindo do reconhecimento da proteção da informação pessoal pela ação de *habeas data* e do princípio fundamental da dignidade humana, é possível ampliar a garantia da inviolabilidade, da intimidade e da vida privada para a proteção de dados pessoais[48].

Defendendo a mesma posição, Sarlet (2020, p. 7) ainda complementa:

> À míngua, portanto, de expressa previsão de tal direito, pelo menos na condição de direito fundamental explicitamente autônomo, no texto da CF, e a exemplo do que ocorreu em outras ordens constitucionais o direito à proteção dos dados pessoais pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade no sentido do que alguns também chamam de uma "intimidade informática".

Ocorre que, em razão da sua natureza, é possível afirmar que o direito à proteção de dados não se enquadra adequadamente ao campo de proteção dos direitos fundamentais previstos na Constituição Federal, apesar da tentativa de esforço nesse sentido. Isso porque os dados tutelados pelo artigo 5º da Lei 13.709/2018 tratam-se, na verdade, de informações pessoais que revelam ou podem revelar aspectos da vida de uma pessoa, identificando-a, mas não necessariamente se caracterizam como íntimos ou relativos à vida privada, numa perspectiva público/privado.

Restringir a proteção de dados pessoais apenas a uma extensão do direito à privacidade seria limitar o seu alcance, simplificando os seus fundamentos. Afinal, conforme aduz Danilo

---

[47] Silva (2005, p. 453) define o *habeas data* como "[...] um remédio constitucional que tem por objetivo proteger a esfera íntima dos indivíduos contra: (a) usos abusivos de registros de dados pessoais coletados por meios fraudulentos, desleais ou ilícitos; (b) introdução nesses registros de dados sensíveis (assim chamados os de origem racial, opinião política, filosófica ou religiosa, filiação partidária e sindical, orientação sexual, etc.); (c) conservação de dados falsos ou com fins diversos dos autorizados em Lei".

[48] Mendes (2018, p. 198) ainda complementa: "Se a CF prevê o *habeas data* como uma garantia processual à disposição do indivíduo para ter acesso ou corrigir os dados que lhe digam respeito, é lógico supor que há um direito material que suporte essa garantia processual: o direito fundamental à proteção de dados ou a autodeterminação informativa, para usar a terminologia consolidada no direito alemão".

Doneda (2011, p. 95), aqui, "outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais". Assim, tendo em vista que a informação pessoal pode circular, ser submetida a tratamento e, em razão disso, sujeitar o seu titular a práticas discriminatórias, os dados mereceriam uma tutela dinâmica desses dados, ultrapassando a esfera do direito à privacidade.

Da mesma forma, a proteção de dados não se amolda à garantia de sigilo da correspondência ou das comunicações[49] nem pode ser analisada somente sob o prisma de uma eventual interceptação, o que levaria, ainda segundo Danilo Doneda (2019, p. 263), a "uma interpretação que não chega a abranger a complexidade do fenômeno da informação pessoal".

Com tais pontos, concorda Mendes (2019, p. 165):

> Vê-se, assim, que embora as garantias de sigilo e de inviolabilidade da intimidade e da privada configurem importantes mecanismos de proteção individual, faz-se necessária uma releitura dessa proteção para lidar com os atuais efeitos do processamento e da utilização da informação sobre o indivíduo. Afinal, essas garantias visam à proteção específica em face de riscos determinados (divulgação de informações íntimas ou interceptação da comunicação, por exemplo) e não abarcam a totalidade dos riscos aos quais o indivíduo está submetido na sociedade da informação.

Por tais razões, por constituir um direito com conteúdo diverso da garantia à privacidade, questiona-se a necessidade de incorporação da proteção de dados ao rol de direitos fundamentais previstos na nossa Constituição Federal, debate que ganhou força após a edição da Lei 13.709/2018 e, posteriormente, com a proposta de Emenda à Constituição nº 17, de 2019, já aprovada no Senado Federal e encaminhada à Câmara dos Deputados para votação.

A referida PEC 17/2019 visa o acréscimo do inciso XII-A ao artigo 5º e do inciso XXX ao art. 22, da Constituição Federal, a fim de incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. De acordo com o texto inicial dessa proposta, tais dispositivos passariam a vigorar com as seguintes redações:

> Art. 5º […]
> XII – A – é assegurado, nos termos da lei, **o direito à proteção de dados pessoais, inclusive nos meios digitais**.
> Art. 22. […]
> **XXX – proteção e tratamento de dados pessoais.** (BRASIL, 2019ª, grifo nosso)

[49] Para Mendes (2014b, p. 165), "O sigilo não parece ser o instrumento mais adequado para resolver os problemas apresentados nessas hipóteses. Afinal, não se trata de tornar sigilosas informações que podem causar a discriminação ou a limitação da liberdade pessoal, mas de regular os efeitos das informações da sociedade, por meio da regulação de seu fluxo e da instituição de procedimentos de controle".

De qualquer maneira, independente da aprovação ou não da PEC 17/2019, já é assente na doutrina e em algumas jurisprudências pátrias a ideia de que a proteção de dados se trata de um direito autônomo que demandaria uma tutela constitucional específica, principalmente diante dos riscos à violação de outros direitos fundamentais que envolvem o processamento e a utilização dos dados pessoais.

Essa dissertação se propõe, então, a traçar uma estrutura dogmática do direito à proteção de dados, ao delinear seu conteúdo e alcance sob a perspectiva da teoria dos direitos fundamentais, tendo, ainda, como parâmetro os conceitos dispostos na Lei de Proteção de Dados, a fim de analisar se é possível afirmar que estamos diante de um direito fundamental que merece expressa guarida na nossa carta constitucional.

3.1 A estrutura dogmática de um direito fundamental à proteção de dados

3.1.1 Um direito fundamental implícito

Em que pese a habitual distinção, na doutrina, entre as expressões "direitos humanos" e "direitos fundamentais" – não sendo objeto desse estudo adentrar na seara terminológica –, é possível afirmar que os direitos fundamentais – termo que será utilizado no presente estudo – são todos aqueles direitos protetivos, baseados no princípio da dignidade da pessoa humana, que garantem o mínimo necessário para que um indivíduo viva de forma digna numa sociedade administrada pelo Estado.

De acordo com Ferrajoli (1999, p. 37, tradução nossa), os direitos fundamentais:

> São todos aqueles direitos subjetivos que correspondem universalmente a "todos" os seres humanos enquanto dotados do status de pessoas, cidadãos ou pessoas com capacidade de agir; entendido por 'direito subjetivo' qualquer expectativa positiva (de prestações) ou negativa (de não sofrer lesões) ligada a um indivíduo por uma norma jurídica; e por 'status' a condição de um sujeito, prevista também por uma norma jurídica positiva, como pressuposto de sua idoneidade para ser titular de situações jurídicas e/ou autor dos atos que são exercício destas.

A sua positivação, nas palavras de Pérez Luño (p.109 apud SARLET, 2018, p. 37), "[...] é o produto de uma dialética constante entre o progressivo desenvolvimento das técnicas de seu reconhecimento na esfera do direito positivo e a paulatina afirmação, no terreno ideológico, das ideias de liberdade e da dignidade humana", levando os direitos fundamentais, desde então, a diversas transformações, como um reflexo das exigências específicas de cada momento

histórico e conforme a mudança de visão em relação ao ser humano, que deixou de ser feita de forma abstrata e passou a considerá-lo na sua maneira de ser e de estar em sociedade.

Tais transformações se refletiram na multiplicação desses direitos ao longo dos anos, fenômeno que a doutrina denominou de "gerações de direitos fundamentais", o que demonstra a capacidade evolutiva dos direitos fundamentais, que varia segundo o seu contexto histórico. Nesse fenômeno, ao mesmo tempo em novos direitos surgem, outros desaparecem ou até mesmo se modificam[50], conforme mudam as reivindicações da sociedade, os interesses das classes de poder e de acordo com o impacto tecnológico[51].

Os direitos de primeira geração, por exemplo, os primeiros a serem positivados e representados pelo direito à vida, à liberdade, à propriedade e à igualdade, dentre outros, traduzem os direitos do indivíduo em face do Estado, de cunho negativo, uma vez que geram condutas de não intervenção que obrigam ao respeito das liberdades individuais, ao contrário dos direitos de segunda geração, que, por serem fruto dos movimentos sociais reivindicatórios do Século XIX, possuem uma dimensão positiva no sentido de exigir do Estado a promoção da justiça social. Nesse contexto, inserem-se os chamados direitos sociais, que garantem a saúde, a educação, o trabalho, o direito de greve, dentre outros.

Os direitos de terceira geração, por sua vez, destacam-se em relação aos anteriores por consistirem em direitos de titularidade difusa ou coletiva, por vezes até indeterminável, pois não visam a proteção do homem enquanto indivíduo, mas de grupos, tendo como destinatário o próprio gênero humano. Esses direitos, em sua maioria, são reflexos do surgimento de uma sociedade de massa oriunda do desenvolvimento tecnológico e científico que causou profundas mudanças nas relações sociais e econômicas. Dentre eles, está o direito à paz, ao meio ambiente, ao desenvolvimento, o direito de comunicação, do consumidor e de autodeterminação dos povos.

Bonavides (2006, p. 80), ao se posicionar sobre os direitos de terceira geração, cita os seguintes termos:

---

[50] Na visão de Sarlet (2018, p. 45), "[...] a mutação histórica experimentada pelos direitos fundamentais, com o reconhecimento progressivo de novos direitos fundamentais, tem o caráter de um processo cumulativo de complementaridade, e não de alternância", não podendo se falar em substituição de uma geração por outra.

[51] Nesse sentido, Bobbio (2004, p. 9) afirma que "[...] os direitos do homem, por mais fundamentais que sejam, são direitos históricos, ou seja, nascidos em certas circunstâncias, caracterizadas por lutas em defesa de novas liberdades contra velhos poderes, e nascidos de modo gradual, não todos de uma vez e nem de uma vez por todas". Ele exemplifica: "a liberdade religiosa é um efeito das guerras de religião; as liberdades civis, da luta dos parlamentos contra os soberanos absolutos; a liberdade política e as liberdades sociais, do nascimento, crescimento e amadurecimento do movimento dos trabalhadores assalariados, dos camponeses com pouca ou nenhuma terra, dos pobres que exigem dos poderes públicos não só o reconhecimento da liberdade pessoal e das liberdades negativas, mas também a proteção do trabalho contra o desemprego [...]".

> Com efeito, um novo pólo jurídico de alforria do homem se acrescenta historicamente aos da liberdade e da igualdade. Dotados de altíssimo teor de humanismo e universalidade, os direitos da terceira geração tendem a cristalizar-se no fim do século XX enquanto direitos que não se destinam especificamente à proteção dos interesses de um indivíduo, de um grupo ou de um determinado Estado. Tem primeiro por destinatário o gênero humano mesmo, num momento expressivo de sua afirmação como valor supremo em termos de existencialidade concreta.

Nesse ponto, ao privilegiar direitos transindividuais e, assim, ampliar o conceito de dignidade humana, pode-se inferir que a terceira dimensão dos direitos fundamentais busca reafirmar o caráter universal do indivíduo, protegendo-o dos riscos causados por determinados regimes políticos e pelos progressos tecnológicos que levaram ao processamento da informação, por exemplo[52].

Inclusive, Sarlet (2018, p. 49) considera que, nessa perspectiva, assume especial relevância "[...] o direito de informática (ou liberdade de informática), cujo reconhecimento é postulado justamente em virtude do controle cada vez maior sobre a liberdade e intimidade individual mediante bancos de dados pessoais, meios de comunicação, etc". No entanto, esse autor ressalta que, "[...] em virtude da vinculação desse direito com os direitos de liberdade (inclusive de expressão e comunicação) e as garantias da intimidade e privacidade [...]", não seria possível afirmar, ao certo, que o direito de informática – e por consequência, enquadrar-se-ia nessa categoria a proteção de dados – estaria dentre os direitos fundamentais de terceira dimensão, até mesmo porque, segundo esse jurista, tem-se observado uma tendência à revitalização de clássicos direitos fundamentais da primeira geração na atualidade em razão das novas formas de agressão aos valores por eles já incorporados.

Nesse contexto, Sarlet (2018, p. 53, grifo nosso) acaba por citar os dados pessoais:

> Na esfera do direito constitucional interno, esta evolução se processa habitualmente não tanto por meio da positivação destes "novos" direitos fundamentais no texto das Constituições, mas principalmente em nível de uma transmutação hermenêutica e da criação jurisprudencial, no sentido do reconhecimento de novos conteúdos e funções de alguns direitos já tradicionais. Com efeito, basta aqui uma referência ao crescente controle do indivíduo por meio dos recursos de informática, **tais como redes e bancos de dados pessoais**, novas técnicas de investigação na esfera do processo penal, avanços científicos (...), bem como as ameaças da poluição ambiental, apenas para nos atermos aos exemplos mais habituais.

[52] Na doutrina, é comum alguns autores defenderem a existência de direitos de quarta geração e até quinta geração, que seriam também uma consequência dos conflitos jurídicos advindos da globalização e das transformações sociais e econômicas decorrentes do desenvolvimento de novas tecnologias. No entanto, essas novas dimensões de direito fundamentais ainda não obtiveram o devido reconhecimento pelo direito pátrio.

E foram justamente as ameaças advindas da coleta e do processamento dos dados pessoais que levou, em alguns países, como já explanado, ao reconhecimento do direito à autodeterminação informativa como direito fundamental do cidadão, mesmo que implicitamente, haja vista a possibilidade de discriminação e danos causados pela circulação de informações que extrapolam o núcleo da privacidade do indivíduo.

É o que se depreende, por exemplo, do seguinte trecho do acórdão nº 76/2019 do Tribunal Constitucional Espanhol, ao reconhecer que, mesmo implícito, o direito à proteção de dados, cujo conceito está intrinsecamente ligado ao direito à autodeterminação informativa, é considerado um direito fundamental pela Constituição espanhola:

> Los diversos instrumentos jurídico-internacionales que alega el Defensor del Pueblo, si bien "no constituyen canon para el enjuiciamiento de la adecuación a la Constitución de normas dotadas de rango legal" (por todas, STC 140/2018, de 20 de diciembre, FJ 6), pueden tener relevancia a la hora de interpretar las disposiciones que sí integran el parámetro de constitucionalidad. Como hemos declarado reiteradamente a lo largo de nuestra jurisprudencia, las disposiciones de los acuerdos internacionales sobre derechos humanos válidamente celebrados y publicados oficialmente en España constituyen, a tenor del art. 10.2 CE, valiosos criterios hermenéuticos del sentido y alcance mínimo de los derechos y libertades que la Constitución reconoce. De suerte que los mencionados instrumentos normativos pueden ser tenidos en cuenta, y lo serán más adelante, para corroborar el sentido y alcance del específico derecho fundamental que ha reconocido nuestra Constitución en orden a la protección de los datos personales. (STC, on-line, 2019).

De qualquer forma, é possível afirmar que o fato de um direito fundamental não estar positivado não implica na sua inexistência, principalmente se este for compreendido na sua fundamentalidade material, no sentido de que, mesmo estando fora do catálogo, ele pode ser equiparado a um direito formalmente fundamental, em razão do seu conteúdo e da sua importância bem como diante de uma análise do contexto social, político e econômico do Estado, o que é feito mediante critérios hermenêuticos e uma construção dogmática que considera a realidade constitucional vigente[53].

No Brasil, o reconhecimento desses direitos fundamentais "implícitos" remete à previsão constante do art. 5º, § 2º, da nossa Constituição Federal, que aduz que "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do

[53] Segundo Hesse (2009, p. 89), a Constituição não pode ser considerada como um sistema fechado, sendo aceitável que possua lacunas a serem preenchidas de acordo com as mudanças históricas, políticas e sociais, devendo sempre estar sempre aberta a modificações. Ele ainda complementa: "Se a Constituição quer ensejar a resolução das múltiplas situações críticas historicamente mutantes, seu conteúdo terá de permanecer, necessariamente, 'aberto ao tempo'".

Brasil seja parte", de onde se depreende ser possível a identificação de novos direitos fundamentais[54], não sendo esse rol, portanto, taxativo, o que revela verdadeira norma inclusiva.

De acordo com Sarlet (2018, p. 82) esse dispositivo constitucional trata da existência de duas espécies de direitos fundamentais, que são "[...] os direitos formal e materialmente fundamentais (ancorados na Constituição formal), e os direitos apenas materialmente fundamentais (sem assento no texto constitucional)", só se concebendo a verificação dessa fundamentalidade material a partir da análise do conteúdo e do alcance do direito em questão.

Assim, sendo possível afirmar que a Constituição Federal adotou um sistema aberto de direitos fundamentais que podem ser deduzidos, já que não previstos expressamente, é razoável considerar o direito à proteção de dados como tal, uma vez que, conforme afirma Mendes (2019, p. 171), a fundamentalidade supracitada "[...] decorre da sua referência a posições jurídicas ligadas ao valor da dignidade humana [...]", tendo em vista que os direitos fundamentais, de forma geral, estão intrinsecamente vinculados ao princípio da dignidade da pessoa humana que norteia a nossa Carta Maior.

Nesse aspecto, pontua Navarro (2011, p. 18):

> Nessa condição, o princípio da dignidade da pessoa humana é princípio reitor, vinculante, que em conjunto com os demais princípios constitucionais possui força normativa, imediata, e ilumina a interpretação de todo o texto constitucional, bem como a aplicação das suas normas. Também encontra amparo nos expressos direitos à intimidade, à privacidade, à inviolabilidade de domicílio, ao sigilo das comunicações, ao acesso à informação e ao devido processo legal, com os quais está estritamente vinculado.

Assim, dentro desse contexto, o direito à proteção de dados, quando analisado à luz da Constituição Federal, acaba por demonstrar a sua fundamentalidade material, uma vez que seu conteúdo está diretamente ligado à dignidade da pessoa e à tutela da personalidade do indivíduo contra o uso indevido dos seus dados, possuindo nítido caráter protetivo da privacidade e da intimidade. É o que se depreende da leitura do art. 2º, inciso VII, da Lei Geral de Proteção de Dados, *in verbis:*

> Art. 2º. A disciplina da proteção de dados pessoais tem como fundamentos:
> […]

[54] Sobre esse ponto, Sarlet (2018, p. 490) lembra que "a categoria dos direitos implícitos pode corresponder também – além da possibilidade de dedução de um novo direito fundamental com base nos constantes do catálogo – a uma extensão (mediante o recurso à hermenêutica) do âmbito de proteção de determinado direito fundamental expressamente positivado, cuidando-se, nessa hipótese, não tanto da criação jurisprudencial de um novo direito fundamental, mas, sim, da redefinição do campo de incidência de determinado direito fundamental já expressamente positivado". E é justamente uma redefinição do campo de incidência do direito à privacidade, expresso na Constituição, que faz com que parcela da doutrina entenda ser o direito à proteção de dados uma extensão daquele direito.

> VII - **os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais**. (BRASIL, 2018, grifo nosso)

Ou seja, essa legislação, ao mesmo tempo em que tem o intuito de promover o desenvolvimento econômico e tecnológico através da regulamentação da coleta e dos dados pessoais, busca também proteger os direitos humanos e a personalidade da pessoa natural[55], revelando, assim, forte preocupação com o indivíduo nesse processo, o que fica evidente também com a previsão, no inciso I desse mesmo dispositivo, da autodeterminação informativa como fundamento também da proteção de dados.

Outrora reconhecida como direito fundamental pelo Tribunal Constitucional alemão, ela também emana do princípio da dignidade da pessoa humana, uma vez que diz respeito à liberdade do indivíduo para dispor sobre suas informações pessoais e determinar a utilização dos seus dados, o que envolve um processo complexo de participação do cidadão no contexto da proteção dos seus dados, consistindo, assim, o direito à autodeterminação num requisito para a liberdade num Estado Democrático de Direito.

O enfoque no indivíduo ainda se verifica com a previsão do consentimento, no artigo 5º, inciso XII, da Lei 13.709/2018, que esse diploma legal denomina como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", sendo esse um dos principais vetores da Lei Geral de Proteção de Dados, uma vez que o termo é mencionado repetidas vezes em outros dispositivos. Inclusive, o seu artigo 7º, inciso I, afirma que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular.

Essa proteção da personalidade no ambiente digital é enfatizada por Costa e Oliveira (2019, p. 35):

> Os princípios que embasam a LGPD demonstram uma centralidade na proteção do ser humano e de sua personalidade. Nesse sentido, o consentimento torna-se central em grande parte dos processos de tratamentos de dados pessoais, o que revela uma preocupação do legislador com a participação do indivíduo no fluxo de suas informações pessoais.

[55] Por se tratar de direitos inerentes ao ser humano e que tutelam o homem das agressões que afetam a sua personalidade, os direitos de personalidade também assumiriam a condição de direitos fundamentais implícitos, em função da sua relação direta com o princípio da dignidade da pessoa humana, sendo essa leitura civil-constitucional decorrente do fato de a pessoa ter se tornado o centro da tutela jurídica. Inclusive, como já explanado no capítulo anterior, é possível afirmar que os dados pessoais são uma extensão da personalidade, uma vez que constituem elementos que compõem a nossa singularidade e permitem a identificação de atributos do indivíduo, vulneráveis a vários riscos e discriminação.

Através de uma análise dinâmica da Constituição Federal, seria possível afirmar ainda que a proteção da personalidade contra o uso indevido dos dados se dá mediante outras garantias constitucionais, quais sejam a da inviolabilidade da intimidade e da vida privada bem como do *habeas data*, permitindo, conforme preleciona Sarlet (2018, p. 90), uma redefinição do campo de incidência de tais direitos fundamentais já expressamente positivados, utilizando-se o recurso da hermenêutica, a fim de traçar uma estrutura dogmática do direito à proteção de dados.

Ocorre que, como tais garantias têm âmbitos de proteção específicos, elas não se mostram suficientes para proteger os indivíduos dos inúmeros efeitos e riscos que envolvem o tratamento de dados, principalmente aqueles que se encontram em bancos de dados informatizados, em função da facilidade de acesso, de transmissão e cruzamento dessas informações, o que, segundo Sarlet (2020, p. 181), "[...] potencializa as possibilidades de afetação de direitos fundamentais das pessoas, mediante o conhecimento e o controle de informações sobre a sua vida pessoal, privada e social"[56].

Por isso, diante desse contexto, a inserção da proteção de dados como um direito fundamental autônomo se justificaria, uma vez que, até então, as informações pessoais não são objeto imediato de tutela constitucional, embora, importante lembrar, o uso indevido destas possam gerar a violação de outros direitos fundamentais.

Nesse mesmo sentido, complementa Mendes (2014b, p. 166):

> Entendemos, assim, que, para manter a atualidade da proteção constitucional do indivíduo em face dos novos desafios sociais e tecnológicos, faz-se necessário interpretar a Constituição de modo a se extrair uma garantia geral de proteção da informação pessoal, que complementaria o atual sistema de garantias específicas do sigilo e da intimidade e da vida privada. Isto é, somente com o reconhecimento de um direito fundamental à proteção de dados pessoais, poderia fazer jus aos atuais riscos aos quais os indivíduos estão submetidos.

Assim, tais aspectos autorizariam, em princípio, o reconhecimento do direito à proteção de dados como direito fundamental implícito, conforme autoriza o artigo 5º, parágrafo 2º, da Constituição Federal[57] (BRASIL, 1988), e forneceriam base ainda para uma previsão expressa

---

[56] Esse mesmo autor ainda lembra que "[...] o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a determinada pessoa natural, sendo irrelevante à qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática". E ainda complementa: o direito à proteção de dados vai além da tutela da privacidade, cuidando-se, de tal sorte, de um direito fundamental autônomo, diretamente vinculado à proteção da personalidade. SARLET (2020, p. 191).

[57] Nesse ponto, Sarlet (2018, p. 89) ressalta que, apesar de à legislação ordinária caber o papel de concretizar e regulamentar os direitos fundamentais positivados na Constituição, sendo apenas esta a fonte de direitos materialmente fundamentais, é razoável a admissão de uma interpretação extensiva no sentido de permitir que a legislação infraconstitucional promova a abertura material do catálogo, o que ocorre quando ela revela posições jurídicas pioneiras, antes mesmo da constitucionalização do direito. Esse raciocínio poderia, assim, ser estendido

desse direito no rol do referido dispositivo constitucional, tal como propõe a PEC 17/2019 (BRASIL, 2019a), dada sua significância para os fenômenos sociais e econômicos e considerando que seu objeto de tutela se distancia do alcance do direito à privacidade, consistindo em direito autônomo com conteúdo específico, mas diretamente vinculado ao princípio da dignidade da pessoa humana, fonte de todos os direitos fundamentais.

Partindo, pois, desse pressuposto, o presente estudo busca construir uma dogmática própria de um direito fundamental à proteção de dados, analisando o seu conteúdo sob uma perspectiva constitucional, mas utilizando também os preceitos trazidos pela Lei 13.709/2018, que desenvolveu seus princípios e fundamentos, a fim de verificar a presença de decisões fundamentais sobre a estrutura do Estado e da sociedade que demonstrem a sua fundamentalidade material.

3.1.2 A dupla perspectiva de um direito fundamental à proteção de dados

Os direitos fundamentais, de forma geral, afirmam-se como núcleo da proteção da dignidade da pessoa humana, sendo a sua evolução e sedimentação frutos de um processo histórico e social que faz com que a estrutura normativa desses direitos se distancie de uma certa homogeneidade, uma vez que variam no tempo e no espaço de acordo com a exigência de cada época.

Essa dinamicidade dos direitos fundamentais aponta para a possibilidade, já consagrada pelo artigo 5º, parágrafo 2º, da Constituição Federal, de existência de direitos fundamentais não escritos ou implícitos das normas do catálogo, tornando a nossa Carta Magna um sistema aberto e indeterminado, sempre apto a resolver as situações críticas que se apresentam diante das mudanças históricas.

Inclusive, sobre essa possibilidade, Bobbio (2004, p. 9) afirma:

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

à Lei 13.709/2018, que inaugurou, no Brasil, os fundamentos e os princípios do direito à proteção de dados com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade do cidadão, mostrando-se, assim, fundamental para toda a sociedade.

Ao afirmar que toda Constituição deve extrair da historicidade os elementos para a formação de um modelo de Estado Constitucional, Hesse (2009, p. 13) também ensina que

> Toda Constituição é Constituição no tempo; a realidade social, a que são referidas suas normas, está submetida à mudança histórica e esta, em nenhum caso, deixa incólume o conteúdo da Constituição. Deixar de observar a mudança histórica leva à petrificação da Constituição que, em curto ou longo período, deixará de cumprir suas tarefas.

Essa realidade histórica viva acaba se apresentando, portanto, como um pressuposto para que a Constituição possa cumprir as funções nela assinaladas e, assim, regular toda a convivência em sociedade, atendendo aos diversos interesses e aspirações de cada geração.

Entretanto, por vezes, torna-se difícil a tarefa de identificação desses novos direitos pelo intérprete, o que demanda a utilização de recursos hermenêuticos com vistas a alcançar a efetivação dos ideais democráticos previstos pela Constituição e, dessa forma, garantir a proteção da dignidade da pessoa humana, fundamento de todos os direitos fundamentais.

É possível, assim, afirmar que somente com a compreensão do conteúdo da norma, a partir das circunstâncias políticas, sociológicas, históricas e da realidade fática que a envolve, é possível concretizá-la. Isso porque "A Constituição é um contínuo processo de interpretação e atualização do texto constitucional, promovida por todos aqueles que fazem o meio no qual está inserido" (HÄBERLE, 1997, p. 73).

Com o direito fundamental à proteção de dados não é diferente, ainda mais se o considerarmos um direito implícito cuja fundamentalidade material se demonstra através da análise do seu conteúdo e do seu âmbito de proteção à luz da Constituição brasileira, fazendo parte desse processo interpretativo ainda a verificação dos seus efeitos sociais, nesse caso causados pela constante evolução das tecnologias que tem permitido a coleta, o tratamento e a transferência dos dados pessoais dos cidadãos sem a observância de princípios gerais de proteção de seus titulares.

Esse uso indevido dos dados pessoais, capaz de ocasionar a violação de outros direitos fundamentais, tais como a liberdade, a privacidade, a intimidade e o livre desenvolvimento da personalidade humana, também se mostra essencial para a caracterização do direito à proteção de dados pessoais como fundamental, uma vez que gera um dever de proteção pelo Estado contra os riscos decorrentes dessa conduta, demandando medidas rigorosas e eficazes de tutela.

Por outro lado, ele enseja ainda um direito de defesa que se torna oponível em face do Estado e também do particular, permitindo que o indivíduo exija um dever de abstenção e de não intervenção no bem jurídico protegido, nesse caso os seus dados pessoais e a sua

privacidade, podendo-se também configurar num direito à prestação, de caráter positivo, na medida que ao cidadão é conferido o direito de obter uma ação positiva do Estado que assegure materialmente ou juridicamente o exercício do seu direito, de ver protegidos os seus dados pessoais.

Tais aspectos acabam por revelar, assim, a dupla perspectiva do direito fundamental a proteção de dados, uma objetiva e outra subjetiva, conforme afirma Mendes (2014b, p. 176):

> O direito fundamental à proteção de dados enseja tanto um direito subjetivo de defesa do indivíduo (dimensão subjetiva) como um dever de proteção estatal (dimensão objetiva). Na dimensão subjetiva, a atribuição de um direito subjetivo ao cidadão acaba por delimitar uma esfera de liberdade individual que não pode sofrer intervenção do poder estatal ou privado. A dimensão objetiva representa a necessidade de concretização e delimitação desse direito por meio da ação estatal, a partir da qual surgem deveres de proteção do Estado para a garantia desse direito nas relações privadas.

Dessa forma, a verificação da fundamentalidade do direito à proteção de dados também passa pela análise dessa dupla dimensão, que demonstra que esse direito exerce diversas funções na ordem jurídica, "[..] o que deflui tanto das consequências atreladas à faceta-jurídico-objetiva, quanto da circunstância de existir um leque de posições jurídico-subjetivas que, em princípio integram a assim denominada perspectiva subjetiva" (SARLET, 2018, p. 161).

Convém registrar, entretanto, que essa multifuncionalidade como critério de classificação dos direitos fundamentais remete à teoria dos quatro *status* desenvolvida por Georg Jellinek, para quem *status* seria a situação em que se encontra o cidadão frente ao Estado, em relação a seus direitos fundamentais. Segundo esse publicista alemão, o indivíduo, enquanto vinculado a determinado Estado como sujeito de deveres e titular de direitos, pode se colocar diante de quatro posições: a) *status* passivo; b) *status* negativo; c) *status* positivo; d) *status* ativo.

No *status* passivo ou *status subjectionis*, o indivíduo encontra-se em posição de subordinação ao poder estatal e, em razão disso, torna-se apenas mero detentor de deveres em reação ao Estado, que, por sua vez, vincula o indivíduo por meio de mandamentos e proibições. Assim, esse *status* não contempla direitos, apenas deveres de submissão. "Em algumas situações, é possível cogitar de restrição de direitos fundamentais, tendo em vista acharem-se os seus titulares numa posição singular diante dos Poderes Públicos" (MENDES, 2020, p. 190).

Já o *status* negativo consiste na ideia de que o poder estatal é juridicamente limitado, uma vez que cabe ao indivíduo gozar de um espaço de liberdade imune às intervenções do

Estado, que passa a ter, nesse caso, o dever de não interferir, de abster-se (ação negativa). Por tal razão, podem os cidadãos, em caso de ingerências, exigir que estas sejam eliminadas, configurando o *status* negativo, assim, um direito de defesa. "Este estado é conformado e assegurado por via dos direitos fundamentais, quando e na medida em que eles, como *direitos de defesa*, protegem determinadas liberdades ou bens jurídicos contra as ingerências, restrições, limitações ou violações do Estado" (PIEROTH; SCHLINK, 2011, p. 60, grifo do autor).

O *status* positivo (*status libertatis)*, por seu turno, assegura ao indivíduo o direito de exigir do Estado que este atue positivamente em seu favor, de forma concreta e eficaz com vistas a satisfazer suas necessidades, o que pode ocorrer através de uma obrigação de dar ou fazer. "Este estado encontra-se conformado e assegurado nos direitos fundamentais quando e na medida em que sejam *direitos de reivindicação, de proteção, de participação, de prestação e de procedimento"* (PIEROTH; SCHLINK, 2011, p. 61, grifo do autor).

Ressalta-se ainda que o exercício dos direitos fundamentais de *status* positivo, quando envolvem prestações estatais, pode ocorrer de duas maneiras: como prestações materiais, através do oferecimento de bens ou serviços aos cidadãos, a exemplo dos direitos sociais[58], ou na forma de prestações normativas, mediante a criação de normas jurídicas que tutelam interesses individuais.

Por fim, o *status* ativo pressupõe que o indivíduo, na sua relação com o Estado, é "titular de competências que lhe garantem a possibilidade de participar ativamente da formação da vontade estatal" (SARLET, 2018, p. 163), exercendo o seu poder soberano ao interferir nas decisões políticas da sociedade na qual está inserido. A expressão máxima deste *status* é o exercício dos direitos políticos, como o direito de voto, por exemplo.

Não sendo o propósito desse estudo prolongar o tema nem tecer considerações a respeito das críticas que cerceiam a teoria de Jellinek, é preciso conhecer a sua relevância para o direito constitucional positivo, uma vez que, ao se sujeitar a adequações e releituras que levam em conta as circunstâncias atuais, ela oferece grande contribuição para a classificação dos direitos fundamentais, que muitas vezes se mostra problemática e complexa. Afinal,

> [...] por meio da classificação é possível obter não apenas uma visão global e sistemática sobre o conjunto dos direitos fundamentais, mas também parâmetros objetivos para sua interpretação, enquadramento funcional e até mesmo a determinação do regime jurídico aplicável (SARLET, 2018, p. 165).

[58] De acordo com o artigo 6º da Constituição Federal, são direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância bem como a assistência aos desamparados. Eles visam resguardar direitos mínimos de qualidade de vida aos cidadãos (BRASIL, 1998).

Dessa forma, pretende o presente trabalho analisar o direito fundamental à proteção de dados a partir da sua dupla perspectiva, a fim entendermos a sua multiplicidade de funções na ordem jurídico-constitucional e a sua configuração como um direito subjetivo de defesa (*status* negativo) contra os desvios de finalidade nos atos de coleta, tratamento e transferência de dados pessoais bem como um direito à prestação (*status* positivo), que atribui ao indivíduo o poder de exigir do Estado ações positivas com vistas a proteger suas informações pessoais de quaisquer violações.

3.1.3 A dimensão subjetiva do direito fundamental à proteção de dados

A dimensão subjetiva dos direitos fundamentais se compreende como fonte de posições subjetivas de vantagens, enquanto faculdades e poderes atribuídos aos seus titulares e "[...] corresponde à característica desses direitos de, em maior ou menor escala, ensejarem uma pretensão a que se adote um dado comportamento ou se expressa no poder da vontade de produzir efeitos sobre certas relações jurídicas" (MENDES, 2019, p. 167).

Dessa forma, numa perspectiva subjetiva, os direitos fundamentais podem assumir tanto um caráter negativo como positivo diante da posição que o indivíduo se coloca em relação ao Estado, conforme a teoria do *status* desenvolvida por Jellinek acima explanada.

O caráter negativo se consubstancia na limitação do poder estatal em intervir na esfera jurídica do titular do direito fundamental, permitindo que este exija do Estado um dever de abstenção, de não interferência na sua parcela de liberdade imune ao poder estatal, enquanto o caráter positivo, ao contrário, se perfaz através da exigência de ações positivas ao Estado, a fim de que este crie condições fáticas e jurídicas para o exercício do direito fundamental dos indivíduos.

Por essa razão, a dimensão subjetiva dos direitos fundamentais envolve, ao mesmo tempo, uma omissão e uma ação estatal, fazendo com que estes sempre compreendam duas facetas (negativa e positiva) e assumam ora a condição de direitos de defesa ora de direitos a prestações, não existindo, importante ressaltar, uma dicotomia entre ambos os direitos, uma vez que a predominância entre um e o outro vai depender do caso concreto, o que não elimina a outra dimensão.

Sobre os direitos de defesa, afirma Sarlet (2018, p. 175):

> Os direitos fundamentais – na condição de direitos de defesa – objetivam a limitação do poder estatal, assegurando ao indivíduo uma esfera de liberdade e outorgando-lhe um direito subjetivo que lhe permita evitar interferências indevidas no âmbito de

> proteção do direito fundamental ou mesmo a eliminação de agressões que esteja sofrendo em sua esfera de autonomia pessoal.

Tais direitos sempre se revelam através de ações negativas, consubstanciando-se em direitos à não-realização de intervenções pelo Estado no bem protegido, com vistas a salvaguardar uma esfera de liberdade inviolável dos indivíduos. E conforme complementa Alexy (2006, p. 303), "[...] a esse direito à não-realização de uma intervenção corresponde, como já demonstrado, o dever de não realizar essa intervenção" por parte do poder estatal.

Nesse contexto, é possível inferir, assim, o amplo espectro alcançado pelos direitos de defesa, uma vez que estes abrangem diversas posições jurídicas que os direitos fundamentais buscam proteger contra eventuais abusos do poder público, ainda mais se considerarmos a eficácia dos direitos fundamentais nas relações privadas[59], o que dá ensejo ao surgimento de novos direitos dessa espécie, a exemplo da proteção de dados.

Nesse ponto, faz-se novamente a ressalva de que o direito à proteção de dados é deduzido como um direito fundamental implícito, com base na autorização prevista no artigo 5º, parágrafo 2º, da Constituição Federal, e, no presente estudo, reforça-se a ideia de que sua fonte advém não apenas de outros dispositivos constituições que guardam íntima relação com esse direito, de onde se retira a sua fundamentalidade, mas também da legislação infraconstitucional[60], no caso, a Lei nº 13.709/2018, a Lei Geral de Proteção de Dados, de onde se extrai elementos que o identificam como um direito materialmente fundamental.

Por isso, cabe destacar o objetivo primordial desse diploma legal, que é a proteção dos direitos fundamentais de liberdade e de privacidade bem como o livre desenvolvimento da personalidade da pessoa natural, conforme aduz o seu artigo 1º, que devem ser inclusos, a rigor, dentre os direitos que compreendem a parcela de liberdade dos indivíduos que seria imune à ação estatal e que, por isso, geram um dever de não interferência do Estado.

---

[59] Ao defender a ideia de que os direitos fundamentais não se limitam apenas ao âmbito das relações jurídicas públicas, mas se estendem também às relações privadas, afirma De la Cruz (2002 apud SARMENTO, 2006, p. 206): "Os direitos fundamentais, em sua dupla vertente subjetiva e objetiva, constituem o fundamento de todo o ordenamento jurídico e são aplicáveis em todos os âmbitos de atuação humana de maneira imediata, sem intermediação do legislador. Por isso, as normas de direitos fundamentais contidas na Constituição geram, conforme a sua natureza e teor literal, direitos subjetivos dos cidadãos oponíveis tanto em relação aos poderes públicos como no que tange aos particulares".

[60] Essa posição, já anteriormente exposta na presente dissertação, é amplamente defendida por Sarlet (2018, p. 82), que, ao reconhecer a dificuldade de identificar direitos que reúnam condições para serem considerados materialmente fundamentais, afirma: "Ponto que igualmente merece destaque é o que diz respeito às fontes dos direitos fundamentais fora do catálogo, que, ao menos em princípio, podem ter assento em outras partes do texto constitucional ou residir em outros textos legais nacionais ou internacionais".

Assim, não pode o Estado, sob pena de violar a privacidade e o livre desenvolvimento da personalidade dos indivíduos, utilizar de forma abusiva os seus dados pessoais por meio de operações de tratamento[61] que venham lhes causar qualquer tipo de discriminação ou constrangimento, devendo, ainda, o Estado se abster de usar as informações pessoais como instrumento de poder e controle a partir dos perfis de comportamento (econômico, familiar, político, profissional e de consumo) traçados a partir da coleta ou com o objetivo de tomada de decisões econômicas, políticas e sociais sem a observância dos princípios que são atinentes à matéria de proteção de dados[62].

Esse dever de abstenção do Estado abrange, portanto, não apenas os dados em si, como se pode observar, mas principalmente valores e garantias fundamentais que se encontram insculpidos ou deduzidos da Lei 13.709/2018, o que torna essa legislação verdadeiro "guarda-chuva" de direitos subjetivos, denotando a sua grande importância para a estabilidade da ordem constitucional vigente[63].

Com isso, a privacidade, a intimidade, a honra, a personalidade e, acima de tudo, a dignidade da pessoa humana devem estar sempre a salvos de agressões por parte do Estado e, inclusive, de particulares quando se trata da coleta e tratamento de dados pessoais.

Merece ainda destaque, nesse ponto, o direito do indivíduo de controlar o recolhimento, a utilização e a divulgação das suas informações pessoais bem como acompanhar a atividade estatal a respeito, no exercício da sua autodeterminação informativa, um dos fundamentos da Lei Geral de Proteção de Dados, o que garante, no exercício desse direito de defesa, a possibilidade de oposição ao tratamento de dados[64], que deve ser protegida contra ações impróprias do poder estatal.

Sobre esse aspecto, pontua Mendes (2014b, p. 117):

---

[61] Nos termos do artigo 5º, inciso X, da Lei 13.709/2018, o tratamento de dados compreende "[...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018).

[62] São princípios do direito à proteção de dados, já explorados em capítulo anterior: princípio da publicidade (ou transparência), princípio da exatidão, princípio da finalidade, princípio do livre acesso e princípio da segurança física e lógica.

[63] Nesse sentido, Doneda (2019, p. 265) complementa: "[...] a proteção de dados pessoais é uma garantia de caráter instrumental, derivada da tutela da privacidade, porém, não limitada por esta; ainda, faz referência a um leque de garantias fundamentais que se encontram no ordenamento jurídico brasileiro".

[64] Um aspecto relevante na Lei 13.709/2018 diz respeito à necessidade de consentimento para a coleta e o tratamento de dados do titular, o que se dá em razão da vulnerabilidade e dos riscos a que estão sujeitos os dados após o desenvolvimento de novas tecnologia, principalmente no ambiente virtual. No entanto, convém ressaltar que essa legislação, no seu artigo 7º, parágrafo 4º, dispensa a exigência de consentimento para o tratamento de dados quando estes se tornam públicos pelo próprio titular, devendo, entretanto, serem resguardados os seus direitos e os princípios previstos nessa lei.

> O controle dos seus dados pessoais pelo indivíduo compõe um aspecto essencial da dimensão subjetiva do direito à proteção de dados pessoais. O conceito geral é o de que, a princípio, o titular dos dados deve ter o controle da coleta, processamento, utilização e circulação dos seus dados pessoais. Afinal, tendo em vista que os dados se referem a ele e influenciam a sua esfera de direitos, somente o titular pode determinar a extensão da circulação de seus dados na sociedade.

Da Lei Geral de Proteção de Dados é possível extrair, portanto, diversas posições jurídicas subjetivas (direitos) que devem ser compreendidas e aplicadas em sintonia e conformidade com a Constituição Federal, uma vez que possuem fundamento constitucional implícito. É o que ocorre também com os direitos do titular da proteção de dados previstos no seu artigo 17, que reitera a garantia da proteção dos direitos fundamentais de liberdade, de intimidade e de privacidade, bem como aqueles dispostos no artigo 18 da Lei 13.709/2018. Dentre eles está o direito ao acesso e ao conhecimento dos dados pessoais coletados, à retificação desses dados e do seu apagamento, como um reflexo da liberdade de escolha do indivíduo, que, por essa razão, acabam por constituir normas de competência negativa para o poder estatal.

É o que se depreende do seguinte rol, *in verbis:*

> 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)

Inclusive, Sarlet (2020, p. 196) dispõe a esse respeito:

> [...] mediante uma simples leitura do catálogo que segue, enunciado nos arts. 17 e 18 da LGPD, é possível perceber que em grande medida as posições jurídicas subjetivas (direitos) atribuídas ao titular dos dados pessoais objeto da proteção legal, que concretiza e delimita, em parte, o próprio âmbito de proteção do direito fundamental à proteção de dados, coincidem com o rol de posições jurídico-constitucionais diretamente e habitualmente associadas à dupla função de tal direito como direito negativo (defesa) e positivo (a prestações).

Tais posições jurídicas constituem, portanto, direitos de defesa contra os desvios de finalidade nos atos de captação, tratamento e divulgação de dados pessoais não só por parte do poder público, mas também por particulares, sendo, assim, oponíveis em face do Estado, a quem incumbe um dever ao mesmo tempo de abstenção[65] e de prevenção contra ações lesivas nesse sentido. Entretanto, paralelamente, consubstanciam-se também em direito a prestações, na medida que conferem aos indivíduos o poder de exigir do ente estatal ações positivas que garantam o efetivo exercício de suas liberdades fundamentais, o que remonta à ideia de *status* positivo desenvolvida por Jellinek.

Sobre esse tema, Alexy (2006, p. 442) pontua que os direitos a prestações funcionam como um contraponto aos direitos de defesa e que "todo direito a uma ação positiva, ou seja, uma ação do Estado, é um direito a uma prestação". E apesar de expor o problema conceitual/terminológico que torna polêmica essa classificação, em razão de concepções fundamentais diversas e obscuridades conceituais e dogmáticas fundamentais, esse autor entende que tais direitos devem ser considerados também num sentido amplo, não se restringindo apenas aos chamados direitos sociais[66].

Nesse sentido, é possível afirmar que o direito fundamental à proteção de dados, ao gerar um dever de abstenção por parte do Estado, exige também do poder público uma atuação a fim de garantir a não violação (sua e de terceiros) à intimidade, à privacidade e ao livre desenvolvimento da personalidade dos indivíduos. Implica, portanto, ações efetivas que permitam, por exemplo, que o titular dos dados pessoais tenha o devido conhecimento do tratamento que é feito em suas informações, que ele exerça o direito de acesso e de retificação destes e que exijam ainda a imposição de limites em relação a utilização e transferência desses dados, com vistas a possibilitar que as situações jurídicas abrangidas pelo contexto da proteção de dados se tornem reais e efetivas no seio da sociedade.

Assim, a proteção de dados, enquanto um direito subjetivo e um direito a prestações, forma uma relação tríade entre o seu titular, o Estado e uma ação positiva deste, obrigando o poder público a tomar medidas fáticas benéficas para proteger não somente os dados pessoais, mas também os demais direitos fundamentais reproduzidos na Lei 13.709/2018. Por isso, a

[65] É importante ressaltar, no entanto, que o exercício dos direitos de defesa não implica a exclusão da ação do Estado, tendo o intuito apenas de formalizar e limitar essa intervenção na esfera de liberdade dos cidadãos.

[66] Sobre esse aspecto, Sarlet (2018, p. 194) ainda lembra que "[...] os direitos a prestações abrangem um feixe complexo e não necessariamente uniforme de posições jurídicas, que podem variar quanto ao seu objeto, seu destinatário e mesmo quanto à sua estrutura jurídico-positiva, com reflexo na sua eficácia e efetivação".

relação jurídica correspondente se traduz numa obrigação de fazer ou de dar, perfazendo-se através de prestações fáticas (materiais) e de prestações normativas (jurídicas).

No que tange às prestações jurídicas, estas requerem a adoção de normas jurídicas organizacionais e procedimentais que "deem vida aos direitos fundamentais e prevejam que estas sejam interpretadas de acordo com os direitos fundamentais que as justificam" (MENDES, 2019, p. 160), sendo a edição da Lei 13.709/2018 um reflexo da dimensão positiva do direito fundamental à proteção de dados, posto que se constitui de normas específicas que buscam estabelecer as condições materiais indispensáveis ao gozo efetivo desse direito[67].

Em razão disso, este acaba por configurar também um direito a prestação fática, uma vez que a definição do conteúdo e da extensão da tutela de dados encontram-se garantidas e delimitadas no texto da Lei 13.709/2018[68], cuja aprovação foi necessária para que a proteção de dados pessoais produzisse eficácia plena e exequibilidade no direito pátrio, dada a sua não-inclusão (ainda) no catálogo de direitos fundamentais expressos. Nesse sentido, inclusive, Mendes (2019, p. 161) pontua que "[...] a maioria dos direitos a prestação, quer pelo modo como enunciados na Constituição, quer pelas particularidades do seu objeto, depende da interposição do legislador para produzir efeitos plenos".

Tais prestações fáticas consistem, assim, em todos os direitos materialmente previstos na referida legislação, de onde se extraem direitos subjetivos cujo objeto e dimensão encontram-se perfeitamente delimitados.

E justamente por demandar prestações não apenas fáticas, mas também normativas, o direito à proteção de dados se mostra também como um direito de proteção, que, por sua vez, é um reflexo da dimensão objetiva dos direitos fundamentais, que atribui à dimensão subjetiva um reforço de efetividade, posto que requer a adoção de medidas positivas de proteção contra intervenções do Estado e até de particulares que sejam lesivas à privacidade e à liberdade e ao livre desenvolvimento da personalidade do cidadão, conforme se demonstrará no tópico a seguir.

---

[67] Impende ressaltar que a edição dessa lei específica não impede o seu diálogo com demais leis brasileiras que também dispõem sobre proteção de dados, tais como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação e o Marco Civil da Internet (BRASIL, 2011).

[68] Ao defender que os direitos a prestação material dependem, necessariamente, de leis e de políticas sociais que os garantam e os definam, Andrade (1987, p. 249 apud MENDES, 2019, p. 163), afirma: "[...] em se tratando de direitos a prestação, o dever imediato que toca ao Estado é precisamente, em primeira linha, o dever de legislar, já que a feitura de leis é a tarefa devida (no caso dos direitos a prestações jurídicas) ou a condição organizatória necessária (no caso dos direitos a prestações materiais)".

3.1.4 A dimensão objetiva do direito fundamental à proteção de dados

Sob uma perspectiva objetiva, os direitos fundamentais "[...] constituem decisões valorativas de natureza jurídico-objetiva da Constituição, com eficácia em todo o ordenamento jurídico e que fornecem diretrizes para os órgãos legislativos, judiciários e executivos" (SARLET, 2020, p. 198), consistindo, nesse aspecto, numa espécie de reforço da proteção dos direitos subjetivos. Aqui, frisa-se, não há uma substituição da dimensão subjetiva, mas uma complementação, uma vez que, na dimensão objetiva, verifica-se uma operatividade prática com a finalidade de assegurar o exercício dos direitos fundamentais.

Isso faz com que as normas de direitos fundamentais adquiram uma função autônoma, transcendendo à sua perspectiva subjetiva, principalmente pelo fato de, sob esse prisma, estarem voltadas para a promoção e proteção desses direitos de toda a comunidade e sociedade, sem visar apenas a defesa do indivíduo, o que torna esses direitos fundamentais, na sua dimensão objetiva, também direitos transindividuais, a exemplo da proteção de dados[69].

Como resultado dessa visão jurídico-objetiva, é possível reconhecer a eficácia irradiante dos direitos fundamentais sobre toda a ordem jurídica, pois, por estarem no topo do sistema jurídico, eles acabam se projetando por todo o ordenamento, influenciando e afetando, inclusive, as relações jurídicas privadas, servindo como critério de interpretação e aplicação do direito infraconstitucional e abrindo ainda espaço para uma interpretação conforme aos direitos fundamentais, à semelhança do recurso hermenêutico de interpretação conforme à Constituição.

Dentre os desdobramentos dessa perspectiva, está também "[...] o dever do Estado não apenas de se abster de intervir no âmbito de proteção desses direitos, mas também de proteger esses direitos contra a agressão ensejada por atos de terceiros" (MENDES, 2014, p. 6), fazendo com que o Estado evoluísse da posição de adversário para guardião desses direitos.

Surgem, assim, daí os chamados deveres de proteção, que resultam "na instituição de deveres vinculantes (juridicamente exigíveis) por parte dos poderes públicos no sentido de proteger as pessoas contra violações dos seus direitos por parte do próprio Estado e dos particulares" (SARLET, 2018, p. 155), fazendo com que tais deveres se consubstanciem também em direitos de proteção, cuja tutela se concretiza mediante a edição de normas que

[69] Como forma de reforçar a natureza jurídica de direito coletivo da proteção de dados, remete-se aqui ao disposto no artigo 81, inciso II, da Lei nº 8.078/1990 (CDC), que afirma serem interesses ou direitos coletivos os "transindividuais, de natureza indivisível de que seja titular grupo, categoria ou classe de pessoas ligadas entre si ou com a parte contrária por uma relação jurídica base" (BRASIL, 1990). Frisa-se, no entanto, a possibilidade de a tutela de dados incidir em outra espécie de direito coletivo, a depender das nuances do caso concreto.

dispõem sobre procedimento administrativo ou judicial, de atos administrativos ou até mesmo através da atuação concreta dos entes estatais.

Nesse sentido, tendo em mente que a proteção de dados pessoais visa conferir ao indivíduo a ingerência e manejo na administração de seus dados pessoais, pode-se considerar a edição da Lei 13.709/2018 como importante instrumento de proteção decorrente dessa perspectiva objetiva dos direitos fundamentais, sendo possível observar nesse diploma não só medidas de caráter preventivo contra os riscos do uso indevido dos dados como também medidas positivas que visam garantir a fruição desse direito fundamental implícito e dos demais direitos fundamentais a ele correspondentes, como o direito à privacidade, à intimidade e à liberdade.

Como primeiro exemplo dessa tentativa de proteger ou menos reduzir as vulnerabilidades a que o indivíduo está sujeito dentro desse contexto, está a exigência do consentimento para o tratamento de dados pessoais, legitimando todas as operações dele decorrentes e permitindo que o indivíduo exerça a sua autodeterminação informativa, numa superação da visão patrimonialista que antes considerava os dados como bens jurídicos de livre disposição dos seus titulares.

Com isso, o foco passou a ser a proteção do indivíduo e dos direitos subjetivos, fazendo com que a proteção da privacidade e da intimidade se tornasse proativa, garantindo ao titular pleno conhecimento do uso de seus dados, através de um consentimento que ainda deve se submeter aos princípios atinentes à matéria, que também configuram um sistema de proteção da pessoa, em mais uma demonstração de que o problema dos dados não se limita a questões patrimoniais, tendo em vista os valores e objetivos reconhecidos pela legislação específica.

Dessa forma, deve o tratamento de dados obedecer às finalidades especificadas, não podendo sofrer posterior tratamento incompatível com estas. Deve ainda ser garantida aos titulares a transparência sobre as operações realizadas bem como o livre acesso à consulta e duração do tratamento, não podendo este se destinar a fins discriminatórios ilícitos ou abusivos, além de outras garantias, na forma de princípios, dispostas no artigo 6º, da Lei 13.709/2018.

As condições para um efetivo controle da circulação das informações pessoais ainda são observadas nessa legislação através da previsão de uma esperada transparência em todo o processo de tratamento, que concede ao titular o direito de revogar o consentimento a qualquer momento, de ter acesso e correção de dados incompletos, inexatos ou desatualizados e ainda

de requerer o apagamento destes, garantindo a liberdade de escolha do titular além de um tratamento seguro, de acordo com as finalidades informadas.

Nesse aspecto, é possível afirmar que a autodeterminação informativa, além de se traduzir como a faculdade dada ao particular de determinar e controlar a utilização dos seus dados pessoais, não se encerra com a simples permissão da pessoa para que terceiros coletem suas informações. Ela pressupõe ainda que o indivíduo participe, de modo consciente, de todo o processo de tratamento. "Daí a importância da preocupação constante com a transparência, sem a qual não é possível discernir o uso justo do uso injusto da informação" (FRAZÃO, 2019, p. 108).

O dever de proteção que se depreende do direito à proteção de dados também encontra reflexo na previsão de responsabilidade civil e do ressarcimento de danos em face do controlador ou o operador[70] que causar ao titular dos dados qualquer dano patrimonial, moral, individual ou coletivo no exercício de atividade de tratamento de dados pessoais. O artigo 42 da Lei 13.709/2018 assegura, em razão de eventual prejuízo, efetiva indenização ao titular, que, por sua vez, no curso de processo civil, poderá ter o ônus da prova invertido a seu favor pelo juiz nas situações em que suas alegações forem verossímeis e houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Depreende-se dessa norma, portanto, a atividade de risco que envolve o tratamento de dados, que oportuniza a utilização indevida ou abusiva de informações, causando prejuízos aos titulares, demandando a criação de mecanismos de tutela à pessoa que permitam o controle sobre seus próprios dados[71]. Nesse sentido, Frazão (2019, p. 127) complementa:

> Para tal complexidade, a LGPD brasileira, com forte inspiração no GDPR europeu, adota as premissas e fundamentos necessários para que a proteção dos dados seja instrumento de preservação dos direitos fundamentais e valores mencionados, a fim de contornar, dentro do possível, os efeitos nefastos de um capitalismo cada vez mais baseado na vigilância e na opacidade.

[70] Os incisos VI e VII do artigo 5º dessa Lei conceituam essas expressões, sendo o controlador a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais e o operador a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).

[71] Ressalta-se que a Lei Geral de Proteção de Dados não substitui a aplicação de sanções administrativas, civis ou penais definidas no Código de Defesa do Consumidor e em outras legislações específicas, podendo ainda o titular dos dados se valer do *Habeas Data*, um instrumento de defesa que se destina à obtenção e retificação de informações constantes de bancos de dados governamentais ou de caráter público.

Por tais razões, o estabelecimento de sanções administrativas mostra-se como mais uma medida de proteção ao titular dos dados, à medida que sujeita os agentes de tratamento a diversas penalidades, tais como advertência, multas, bloqueio e eliminação dos dados a que se refere a infração. Além disso, sujeitam-se também esses agentes à suspensão parcial do funcionamento do banco de dados e, inclusive, do exercício da atividade de tratamento dos dados pessoais, o que pode culminar na proibição total ou parcial desse exercício.

Tais sanções, previstas no artigo 52 da Lei 13.709/2018, no entanto, só podem ser aplicadas mediante procedimento administrativo que possibilite a ampla defesa, mas obrigam, de certa forma, os entes responsáveis pelo tratamento de dados a seguirem todas as medidas de segurança necessárias a essa operação.

Os direitos de proteção podem ensejar ainda a criação de órgãos encarregados de dar efetividade a esses deveres de proteção por parte do Estado, a exemplo da previsão da Autoridade Nacional de Proteção de Dados (ANPD) prevista no artigo 55-A a 55-L da Lei 13.709/2018, que consiste em órgão da administração pública federal, integrante da Presidência da República, com autonomia técnica e decisória, que tem, dentre outras atribuições e competências, a função de zelar pela proteção dos dados pessoais bem como fiscalizar e aplicar as sanções supracitadas.

Sobre esse mecanismo de proteção, pontua Mendes (2014b, p. 180):

> A proteção do indivíduo contra a discriminação pelo processamento dos dados pessoais somente pode ser atingida com a proibição ou limitação do armazenamento de informações sensíveis. Ademais, a efetivação do direito fundamental á proteção de dados depende do controle e fiscalização da atividade de processamento de dados por autoridade administrativa, de modo a complementar um sistema judicial de resolução de conflitos.

Dessa forma, decorre da perspectiva jurídico-objetiva do direito fundamental à proteção de dados a ideia de que o Estado, em razão do seu dever de proteção, deve proporcionar aos cidadãos mecanismos que lhes tragam a certeza da concretude de seus direitos, sem os quais seria impossível o estabelecimento de limites em relação à coleta e armazenamento de dados pessoais no contexto da sociedade da informação.

Extrai-se, então, daí a relevância de tais mecanismos como forma de tutela contra as ingerências indevidas não só por parte do ente estatal, mas também por particulares, o que permite, em razão da sua especificidade e complexidade, considerar o direito à proteção de dados um direito materialmente fundamental e autônomo, que tem como objetivo primordial a valorização da pessoa humana.

3.1.5 Titularidade e destinatários do direito fundamental à proteção de dados

O conteúdo jurídico-objetivo dos direitos fundamentais, enquanto direitos individuais, do homem e do cidadão e enquanto um dever de proteção, sugere que eles tenham "[...] por objeto a proteção de domínios concretos, especialmente domínios em perigo da liberdade humana" (PIEROTH; SCHLINK, 2011, p. 68). Essa ideia converge no sentido de que os direitos fundamentais se posicionam sempre como instrumento de proteção ao indivíduo e, ao mesmo tempo, como mecanismo de limite ao poder do Estado com vistas a assegurar os direitos e garantias fundamentais.

Nessa esteira, por estar em conexão com a dignidade da pessoa humana e o livre desenvolvimento da personalidade, o direito fundamental à proteção de dados tem, em primeira linha, como titulares todas as pessoas naturais identificadas e identificáveis, estando a dogmática de proteção de dados brasileira, a exemplo do direito europeu, intimamente ligada à proteção existencial do indivíduo.

Esse entendimento fica claro na leitura do artigo 1º da Lei 13.709/2018, que excluiu claramente do seu âmbito de proteção as pessoas jurídicas:

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

Dessa forma, a despeito de esparsos posicionamentos doutrinários que questionam a titularidade da pessoa jurídica[72], restringe-se esse estudo à consideração de que apenas às pessoas naturais aplicam-se os mecanismos de proteção advindos desse direito materialmente fundamental, diante da ausência de embasamento literário e jurisprudencial nesse sentido. Essa limitação decorre da ideia, portanto, de que o direito à proteção de dados é um direito humano por excelência, cuja preocupação é a tutela das situações existenciais dos titulares de dados.

Não à toa, ele tem sido enquadrado como uma nova espécie de direitos da personalidade, a partir de uma leitura civil-constitucional que busca afastar o direito à proteção

[72] Sarlet (2020, p. 204) suscita essa discussão: "[...] cuida-se, de todo modo, de tema atual e que exige ser levado a sério. Especificamente no que concerne à proteção de dados e considerando que as pessoas jurídicas já são protegidas, inclusive na perspectiva jusfundamental, por outros direitos e garantias (sigilo industrial e comercial, propriedade imaterial etc.), é questionável que a inclusão das pessoas jurídicas no polo subjetivo ativo dos direitos à privacidade e intimidade, bem como do direito à proteção de dados pessoais, implique ganho real qualitativo de proteção".

de dados do arcabouço normativo e conceitual do direito à privacidade, que possui um centro gravitacional diverso daquele. Nesse aspecto, a normatização do direito à proteção de dados

> Não pode ser reduzida a uma mera "evolução" do direito à privacidade, mas encarada como um novo direito da personalidade que percorre, dentre outras liberdades e garantias fundamentais, a liberdade de expressão, de acesso à informação e de não discriminação. Em última análise, trata-se da nossa própria capacidade de autodeterminação (BIONI, 2020, p. 90)

Diferentemente da titularidade, tem-se o destinatário do direito fundamental à proteção de dados, que é "[...] a pessoa (física, jurídica ou mesmo ente despersonalizado) em face da qual o titular pode exigir o respeito, proteção ou promoção do seu direito (SARLET, 2018, p. 215). Isso faz com que não só o Estado, mas também os particulares sejam destinatários desse direito, uma vez que eventuais agressões à intimidade, à privacidade e à liberdade do titular dos dados podem decorrer de ações tanto do poder público como de entes privados ou pessoas físicas.

Assim, num primeiro momento, o direito fundamental à proteção de dados destina-se ao Estado, como reflexo do seu dever de proteção, vinculando o Poder Legislativo, o Poder Executivo e o Poder Judiciário, que devem sempre pautar suas ações e decisões conforme os postulados constitucionais, reconhecendo, assim, a máxima eficácia desse direito fundamental, que retira do seu conteúdo e alcance bem como de valores insculpidos em direitos fundamentais correlatos a sua fundamentalidade material.

Isso faz com que o Poder Legislativo, no exercício da sua competência negativa, proíba a edição de normas que contrariem as finalidades, os princípios e os direitos subjetivos relacionados à proteção de dados e, ao mesmo tempo, revestido do seu *status* positivo, crie e desenvolva normas em conformidade com esse direito fundamental, a exemplo do sistema de garantias materiais e processuais contemplados na Lei 13.709/2018, sendo reflexo desse dever de proteção do Poder Legislativo, como lembra Sarlet (2020, p. 206), a previsão de "[...] eventual criminalização de violações dos direitos fundamentais relevantes em matéria de proteção de dados, a responsabilidade civil de particulares e do Estado, instrumentos processuais adequados, dotação orçamentária suficiente, entre outros".

Da mesma forma, os órgãos do Poder Executivo[73] não podem se furtar a essa vinculação, na medida em que a atuação destes naturalmente se volta para o interesse público

[73] Ressalta-se que aqui a expressão Poder Executivo abrange não só as pessoas jurídicas de direito público, mas também as pessoas de direito privado a quem foram outorgados poderes públicos para tratar com o particular, valendo-se do seu *jus imperium*.

e para o bem-estar da coletividade, o que os obriga a interpretar e executar não só a Lei 13.709/2018, mas também outros diplomas que disciplinam sobre proteção de dados conforme esse direito fundamental, sempre prezando pela preservação da liberdade, da privacidade e do livre desenvolvimento da personalidade dos seus cidadãos diante de situações concretas que envolvam o uso de dados pessoais. Inclusive, a inobservância dessa vinculação, no exercício da atividade discricionária do Poder Executivo, poderá implicar a invalidação judicial desses atos administrativos através do controle jurisdicional.

Ao Poder Judiciário também cabe vincular seus atos jurisdicionais bem como as decisões judiciais conforme o direito fundamental à proteção de dados diante dos casos concretos que se apresentam, sendo ainda um dever dos tribunais a interpretação, a aplicação das leis específicas e a formatação do processo de acordo com os preceitos ditados pela Constituição. Cabe-lhe, inclusive, a declaração de inconstitucionalidade de normas e atos dos demais entes estatais que estejam contrários à Constituição, o que constitui um poder-dever de negar a aplicação de preceitos que desrespeitem esse e quaisquer direitos fundamentais.

Exemplo dessa dimensão negativa dessa vinculação do Poder Judiciário ocorreu em decisão proferida pelo Supremo Tribunal Federal, datada de maio de 2020, que suspendeu a eficácia da Medida Provisória nº. 954/2020 – (BRASIL, 2020), que tratava do compartilhamento de dados pelas empresas de telecomunicação, prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) –, por entender que ela não satisfazia as exigências da Constituição no tocante à efetiva proteção de direitos fundamentais dos brasileiros.

A referida decisão, que será melhor explorada no próximo capítulo dessa dissertação, foi fundamental e paradigmática para a construção de um direito fundamental, autônomo e implícito à proteção de dados, além de reconhecer o direito à autodeterminação informativa. Ela significou, assim, uma clara demonstração de que ao Poder Judiciário também cabe, "por meio da aplicação, interpretação e integração, outorgar às normas de direitos fundamentais a maior eficácia possível no âmbito do sistema jurídico" (MIRANDA, 1993, p. 283-4 apud SARLET, 2018, p. 391).

Assim, de acordo com Sarlet (2020, p.205),

> Tais atores devem, no âmbito e limites de suas respectivas funções, competências e atribuições, aplicar e concretizar o direito à proteção de dados, assegurando-lhe a sua máxima eficácia e efetividade concreta, tanto na condição de direito subjetivo negativo (não intervenção arbitrária no seu âmbito de proteção), quanto, por força de sua dimensão objetiva, levando a sério os respectivos deveres de proteção e o critério da proibição de proteção insuficiente.

Frisa-se que "[...] esse dever de proteção adquire ainda mais relevância em contextos de desequilíbrio de poder entre as partes, nos quais a livre autodeterminação é ainda mais improvável, como ocorre nas relações trabalhistas ou de consumo" (MENDES, 2014a, p. 182), e ainda no contexto da proteção de dados, no qual, em razão do advento de novas tecnologias e do desenvolvimento de bancos de dados, "[...] existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados" (MULHOLLAND, 2018, p.172).

Vivemos, assim, numa sociedade governada por dados, na qual os seus titulares e aqueles que realizam o tratamento desses dados, muitas vezes representados por entes privados detentores de poder social e econômico, estão em permanente conflito gerado por um verdadeiro desequilíbrio de poderes. Daí se extrai o entendimento de que o direito fundamental à proteção de dados não exerce sua eficácia vinculante somente na esfera estatal, mas também nas relações privadas, se considerarmos que ele envolve massivamente atores privados.

Nesse ponto, importa trazer a lição de Sarlet (2018, p. 396):

> [...] No Estado social de Direito não apenas o Estado ampliou suas atividades, mas também a sociedade cada vez mais participa ativamente do exercício do poder, de tal sorte que a liberdade individual não apenas carece de proteção contra os Poderes Públicos, mas também contra os mais fortes no âmbito da sociedade, isto é, os detentores de poder social e econômico, já que é nesta esfera que as liberdades se encontram particularmente ameaçadas.

Assim, sem objetivar o aprofundamento a respeito da intensidade ou extensão do *modus vinculandi* dessa eficácia horizontal do direito fundamental à proteção de dados, tema que mereceria ser objeto de estudo à parte dessa dissertação[74], filia-se à corrente que defende que, enquanto um direito materialmente fundamental, as normas e princípios atinentes à proteção de dados também se aplicam a toda a ordem jurídica, inclusive a privada, não sendo concebível a ideia de que, na atual sociedade da informação, as relações entre particulares estariam desprendidas dessa proteção. Afinal,

> No tocante à proteção dos dados pessoais, seja em que contexto for, mas em especial no ambiente digital, não se pode admitir uma esfera de atuação privada completamente livre dos direitos fundamentais, gerando uma espécie de

[74] De acordo com Alexy (2006, p. 528), essa ideia do efeito horizontal dos direitos fundamentais é amplamente aceita. No entanto, por se tratar de uma relação na qual ambos os polos (cidadão-cidadão) são titulares de direitos fundamentais, ao contrário da relação entre Estado-cidadão, torna-se polêmica a discussão sobre a extensão desse efeito perante terceiros, uma vez que se está diante de um problema de colisão de direitos fundamentais, que demanda, por sua vez, uma questão sopesamento.

> imunidade, tanto mais perigosa – no que concerne a violações de direitos – quanto mais força tiverem os atores privados que operam nesse cenário (SARLET, 2020, p. 209-210)

De qualquer modo, reproduz-se aqui a ideia esposada por Sartlet (2018, p. 401), no sentido de que há, em tais casos, "[...] uma necessária vinculação direta (imediata) *prima facie* também dos particulares aos direitos fundamentais [...]", de onde se depreende – utilizando-se de uma interpretação extensiva – ser o direito fundamental à proteção de dados diretamente aplicável nas relações privadas, que gera também direitos subjetivos oponíveis aos entes privados[75].

Assim, diante de todo o exposto, o presente capítulo buscou apontar a fundamentalidade material que justificaria o direito à proteção de dados enquanto um direito fundamental, buscando construir uma dogmática jurídica adequada à matéria, sem definir de modo fundamentalmente novo o seu conteúdo, mas, dentre as várias interpretações possíveis, preferindo aquela que melhor se conforma à Constituição, que traz valores e garantias fundamentais plenamente compatíveis e correspondentes com aquelas abrangidas pelo direito à proteção de dados.

Passa-se agora a analisar o amadurecimento da matéria no âmbito da jurisprudência brasileira e a interpretação conforme à Constituição dada ao direito à proteção de dados, colaborando para a construção de um direito autônomo, conforme se depreende do capítulo a seguir.

[75] Nesse aspecto, Mendes (2019, p. 179) sustenta que, de acordo com a teoria da eficácia direta ou imediata, "[...] os direitos fundamentais devem ter pronta aplicação sobre as decisões das entidades privadas que desfrutem de considerável poder social, ou em face de indivíduos que estejam, em relação a outros, numa situação de supremacia de fato ou de direito", de onde se depreende haver também, nas relações jurídicas relacionadas ao uso de dados, uma eficácia direta desse direito fundamental implícito, dada a situação de desigualdade econômica e de poder naturalmente existente entre as partes envolvidas.

4 A APLICAÇÃO DO DIREITO À PROTEÇÃO DE DADOS NA JURISPRUDÊNCIA PÁTRIA

4.1 A contribuição das leis setoriais brasileiras

Vivemos na denominada era da informação, na qual o crescimento exponencial de novas tecnologias tem sido o responsável por uma nova forma de organização social e por criar "[...] mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável [...]" (BIONI, 2020, p. 4), contribuindo, inclusive, com novas formas de distribuição de poder na sociedade.

A amplificação dos ambientes digitais demandou o surgimento de novas formas de coleta e tratamento dessas informações, coincidindo com a crescente necessidade de dados por partes de entes públicos e privados e fazendo com que estes dados e as informações dele colhidas passassem a figurar como importante ativo para essas instituições na consecução de suas atividades e objetivos. Como resultado desse fenômeno, houve uma progressiva redução na esfera da privacidade e da intimidade dos indivíduos ocasionada pela preocupante capacidade de manipulação de dados pessoais.

Os riscos provenientes do uso dessas informações, aliados ao crescente fluxo internacional de dados pessoais, gerou, assim, a necessidade de regulamentação da matéria com a criação de instrumentos jurídicos que buscassem fornecer base para o funcionamento adequado das regras de mercado e, ao mesmo tempo, tutelar os dados dos indivíduos e seus direitos fundamentais, uma vez que o grande desafio que se colocou à frente dos cidadãos foi o controle dos seus dados pessoais. Tornou-se, dessa forma, "[...] cada vez mais difícil considerar o cidadão como um simples "fornecedor de dados, sem que a ele caiba algum poder de controle [...]" (RODOTÀ, 2008, p. 36).

Ao Poder Judiciário, à medida que o tema se tornou recorrente nas relações sociais e virtuais, coube equilibrar os diferentes conflitos de interesses, numa situação desafiadora diante da ausência de uma regulação específica até o ano de 2020, quando entrou em vigor da Lei Geral de Proteção de Dados, fazendo com que os casos concretos apresentados até então fossem decididos através da associação do direito à proteção de dados com direitos fundamentais dispostos na Constituição Federal, em especial os direitos à privacidade, à intimidade, ao sigilo de dados e ainda a garantia do *habeas data*.

Além dessa leitura sistemática dos princípios e valores constitucionais, o Poder Judiciário, até o advento da Lei 13.709/2018, contava também com legislações ordinárias que

trazem em seu bojo normas que contemplam a proteção de dados, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e o Marco Civil da Internet, que de alguma forma estabelecem mecanismos de controle sobre os dados, mas de forma fracionada, sem sistematizar a matéria, uma vez "[...] que tendem a se orientar mais pela lógica de seus campos específicos do que por uma estratégia baseada na tutela integral da personalidade através da proteção dos dados pessoais" (DONEDA, 2019, p. 45).

Isso, por vezes, deu margem a decisões equivocadas, que fragilizavam a proteção do indivíduo, como se verifica no caso primeiro caso analisado. Trata-se de uma ação coletiva ajuizada em face da Confederação Nacional de Dirigentes Lojistas – SPC BRASIL, na qual o Ministério Público, autor da ação, aduzia abusividade por parte da ré, que vendia dados e informações pessoais de consumidores, sem prévia anuência, através de sua página virtual, a fim de que estes pudessem ser utilizados em ações de marketing e telemarketing por empresas. Essa comercialização incluía dados como nome completo, telefone, endereço, número de documentos de identificação, data de nascimento, nomes dos pais, e-mail, dentre outras informações pessoais.

Apesar de ação ter sido julgada procedente, em grau de apelação (processo nº 70069420503), o Tribunal de Justiça do Rio Grande do Sul reformou a sentença, por entender que a ação praticada pela ré não era considerada ilícita, tendo em vista que os dados divulgados eram aqueles comumente fornecido por todos os cidadãos comuns, na prática de atos da vida civil, não consistindo em dados sigilosos ou confidenciais. Entendeu ainda esse Tribunal que não estava configurada, portanto, qualquer ofensa à privacidade ou a outro direito fundamental dos consumidores, conforme se depreende da ementa a seguir destacada:

> Apelação cível. Responsabilidade civil. Ação coletiva. SPC BRASIL. Marketing service. Divulgação de dados. Ausência de ofensa a direitos da personalidade. Hipótese em que os dados divulgados não são sigilosos, pois se trata de informação fornecida nas relações negociais cotidianas. Inexistência de dados sensíveis. Apelos providos (TJRS, 2016, on-line).

Frisa-se que tal decisão foi prolatada em 2016, portanto, antes do advento da Lei Geral de Proteção de Dados, tendo sido trazido à tona apenas para que se observe que, na ausência de uma legislação específica e de uma sistematização da disciplina, o Poder Judiciário não dispunha, na época, de critérios para conciliar os diferentes interesses econômicos com a tutela da privacidade e do indivíduo.

Demonstra isso o fato de a decisão ter como fundamento apenas o artigo 43 do Código de Defesa do Consumidor, bem como a Lei do Cadastro positivo, que segundo esse Tribunal,

não proíbem os arquivos de consumo (cadastros e bancos de dados), apenas regulamentam o seu controle.

Ocorre que, no caso concreto, as informações pessoais supracitadas e comercializadas pela ré, conforme prevê a lei 13.709/2018, configuram dados que tornam as pessoas identificadas, de forma clara e inequívoca, ou ao menos identificáveis, devendo, portanto, serem consideradas como um prolongamento da personalidade desses indivíduos, o que, por si só, já impedia o tratamento sem o consentimento destes nos dias atuais.

Ademais, não se suscitou ainda, na referida decisão, a finalidade, a adequação e a necessidade da transmissão dessas informações, além de outros princípios que deveriam ter sido observados pela ré para a proteção dos dados dos consumidores, o que hoje configuraria um ato abusivo, uma vez que viola a privacidade e traz outros riscos ao livre desenvolvimento da personalidade das pessoas envolvidas.

No segundo caso analisado, uma ação de obrigação de fazer e compensação de dano moral, uma pessoa física objetivava a exclusão das suas informações cadastrais do banco de dados mantido por uma empresa, alegando também o uso indevido e a comercialização de suas informações pessoais e sigilosas, mas cujo pedido foi negado pelo juiz de primeiro grau.

Irresignado, o autor da ação recorreu da decisão, tendo, nesse caso, o Tribunal de Justiça de Minas Gerais dado provimento à sua Apelação, levando o Réu, por sua vez, a interpor Recurso Especial (Nº 1.758.799 – MG) junto ao Superior Tribunal de Justiça, com vistas a reformar o acórdão. Em 2017, a Relatora Ministra Nancy Andrighi negou provimento a esse recurso, fundamentando sua decisão com base no Código de Defesa do Consumidor e na Lei de Cadastro Positivo, ao afirmar que, de acordo com o dever de informação, deve o consumidor ser comunicado da abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele, consoante determina o § 2º do art. 43 do CDC, conforme se depreende do seguinte trecho da decisão, *in verbis:*

> Em qualquer das circunstâncias, tem o consumidor o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. [...] A questão se torna ainda mais preocupante diante da possibilidade de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º. [...]. Assim, a inobservância de qualquer dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. (STJ, 2019, on-line)

Dessa forma, utilizando as mencionadas leis setoriais, o Superior Tribunal de Justiça decidiu que o réu deveria excluir os dados do autor de seu banco de dados, fazendo expressa menção ao tratamento e compartilhamento de dados pessoais, ao consentimento do titular e à proteção da pessoa, retificando o equívoco da sentença prolatada pelo magistrado de 1º grau.

Tais leis ordinárias, durante muito tempo, serviram como fundamentos para decisões relacionadas ao tratamento de dados, ora protegendo os indivíduos, ora enfraquecendo seus direitos, tendo esse aparato normativo recebido reforço com a Lei 12.965/2014, conhecida como Marco Civil da Internet, que trouxe amparo a muitas situações relacionadas à privacidade no domínio do uso das tecnologias da informação. E embora não se tratar de uma legislação especifica sobre proteção de dados, suas normas significaram um importante avanço da sua doutrina, contribuindo com os conflitos surgidos no âmbito da Internet e imprimindo um novo significado ao direito à intimidade.

Exemplo disso são as decisões prolatadas nos autos da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403 e da Ação Direta de Inconstitucionalidade (ADI) 5527, que têm em comum o debate sobre a possibilidade de decisões judiciais autorizarem o bloqueio de serviços de mensagens pela internet, como o aplicativo WhatsApp, e o direito das pessoas no ambiente digital, repercutindo, portanto, no direito à proteção de dados. Por possuírem objetos em comum, ambas as ações foram julgadas em conjunto em maio de 2020.

Na Ação Direta de Inconstitucionalidade (ADI) 5527, ajuizada por partido político e que tem como relatora a Ministra Rosa Weber, discutiu-se especificamente a inconstitucionalidade do artigo 10, § 2º, da Lei nº 12.965/2014[76] (Marco Civil da Internet) e do artigo 12, incisos III e IV[77], do mesmo diploma, que têm sido comumente suscitados como fundamento para decisões judiciais que determinam a suspensão temporária de serviços de troca de mensagens na Internet e para o estabelecimento de sanções em caso de descumprimento de ordem judicial que determina a disponibilização do conteúdo dessas mensagens.

---

[76] Afirma essa norma: "A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de **dados pessoais** e do conteúdo de comunicações privadas, devem atender à **preservação da intimidade, da vida privada, da honra e da imagem** das partes direta ou indiretamente envolvidas. [...] § 2º O conteúdo das comunicações privadas **somente poderá ser disponibilizado mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º". (BRASIL, 2020c, grifo nosso)

[77] Aduz o artigo 12 dessa lei: "Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: [...] III - **suspensão temporária das atividades** que envolvam os atos previstos no art. 11; ou; IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11". (BRASIL, 2020c, grifo nosso)

Fazendo remissão ao artigo 7º dessa lei, que assegura a inviolabilidade e sigilo do fluxo das comunicações no ambiente da Internet, e ao artigo 11, que estatui que em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações devem ser respeitados os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros, a relatora Ministra Rosa Weber afirmou que "os aparelhos de telefone móvel guardam muito mais da vida privada e intimidade de seus proprietários do que as portas e paredes, gavetas e armários da residência de cada um deles" (STF, 2020, on-line), devendo ser considerada indevida a invocação de tais dispositivos, uma vez que a Lei nº 12.965/2014 não ampara a prática de bloqueio de aplicativos de mensagens, configurando medidas dessa natureza uma grave restrição à liberdade de expressão.

Ainda de acordo com essa decisão, além do direito à privacidade, à intimidade, à honra e à imagem, merece a personalidade individual também ser protegida, como pressuposto de uma sociedade democrática, devendo tais direitos serem livres de ingerências externas. No entanto, segundo a relatora, ao mesmo tempo em que surgem novas tecnologias de comunicação, adaptam-se as tecnologias voltadas à vigilância, tais como interceptação, raio-x, acesso furtivo a sistemas, desencriptação etc, o que diminui a esfera de proteção da privacidade dos indivíduos. E numa referência também à proteção de dados, afirma a Ministra Rosa Weber:

> Vale observar, ainda, que os maiores desafios contemporâneos à proteção da privacidade nada têm a ver com a imposição de restrições à liberdade de manifestação, enquanto relacionados, isto sim, aos imperativos da segurança nacional e da eficiência do Estado, à proliferação de sistemas de vigilância e à emergência das mídias sociais, **juntamente com a manipulação de dados pessoais em redes computacionais por inúmeros, e frequentemente desconhecidos, agentes públicos e privados**. (STF, 2020, on-line, grifo nosso)

Dessa forma, em situações como essa, deve a Constituição Federal ser adaptada ao mundo digital, a fim de preservar os interesses, os direitos e as liberdades que essa Carta sempre prezou, impondo, assim, restrições a qualquer atuação do Estado que possa diminuir a proteção dos direitos fundamentais dos usuários da rede. Por isso, de acordo com essa decisão,

> [...] não podem a hermenêutica constitucional e o desenvolvimento legislativo ficar alheios a essas mudanças no tempo, tendo em vista a manutenção do equilíbrio entre proteção da privacidade e os limites da atuação do Estado. É que a Constituição, assim como o estado da técnica, institui um conjunto de restrições à atuação do Estado. (STF, 2020, on-line)

Assim, entendeu-se que, como o artigo 5º, XII, da Constituição Federal, deve ser interpretado, segundo precedentes dessa Corte, no sentido de que a lei (a que essa norma se

refere) só pode autorizar a suspensão do sigilo de comunicações privadas para fins de investigação criminal ou instrução processual penal – nesse caso, a atividade legislativa deve atender aos limites impostos pela Constituição – os artigos 7º, II e III, e 10, § 2º, do Marco Civil da Internet, à luz do art. 5º, XII, da Carta Maior, induzem à interpretação também de que a inviolabilidade do sigilo das comunicações no âmbito da internet somente pode ser excepcionada, por ordem judicial, no âmbito da persecução penal, a exemplo do que ocorre com as comunicações telefônicas.

Assim, de acordo com a decisão, "tratando-se de norma restritiva de direito fundamental da personalidade, sua aplicação legítima depende de sua conformidade com o art. 5º, XII, da Constituição: ordem judicial dada no âmbito de investigação criminal ou instrução processual penal" (STF, 2020, on-line).

No entanto, essa interpretação conforme à Constituição não torna, consequentemente, ilegal ou limita o uso da criptografia, recurso tecnológico que protege o sigilo das comunicações realizadas no ambiente da internet, e entender assim configuraria, segundo a relatora, um retrocesso que levaria a tecnologias de comunicação menos seguras e a garantias e liberdades reduzidas apenas para atender às ambições de vigilância do poder estatal. Por isso,

> Em certa medida, a liberdade fundamental que assegura ao indivíduo o direito de fechar o portão de casa com um cadeado, elevar a altura do muro ou pendurar uma cortina na janela, autoriza cogitar uma espécie de direito fundamental à encriptação, ou pelo menos que o uso da criptografia consiste em uma ferramenta indispensável, nos dias de hoje, para assegurar o direito à privacidade (STF, 2020, on-line).

"Trata-se, pois, de tecnologia que atua no sentido da realização material da garantia de preservação do sigilo das comunicações consagrada no art. 5º, XII, da CF" (STF, 2020, on-line) e impedir o seu uso ainda traria sérios riscos à proteção de dados, de acordo com a Ministra Rosa Weber, citando estudo publicado em 2015 pela UNESCO:

> Na medida em que nossos dados possam ser considerados representativos de nós mesmos, a criptografia tem um papel a desempenhar na proteção de quem somos e na prevenção de abuso de conteúdo do usuário. Também permite uma proteção significativamente maior da privacidade e do anonimato em trânsito, garantindo que o conteúdo (e às vezes também os metadados) das comunicações sejam vistos apenas pelo destinatário pretendido. (STF, 2020, on-line).

Ainda de acordo com o voto da referida Ministra, as sanções a que se referem o artigo 12 da Lei nº 12.965/2014 têm como objetivo a proteção da privacidade além de outros direitos dos usuários de Internet, não sendo possível retirar do teor dos incisos III e IV desse dispositivo a fundamentação para decisões judiciais que tenham como objetivo a suspensão do serviço de

comunicação oferecido por aplicativos em caso de desobediência à ordem judicial de fornecimento do conteúdo de comunicações trocadas entre usuários. Trata-se, pois, de "uma norma protetiva dos direitos dos usuários, que de modo algum configura suporte jurídico à imposição de sanções em decorrência do descumprimento de ordem judicial" (STF, 2020, on-line).

Por tal razão, foi julgado improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014 bem como julgado parcialmente procedente o pedido de interpretação dessa norma conforme a Constituição Federal, ficando assentado que

> As penalidades de suspensão temporária das atividades e de proibição de exercício das atividades somente podem ser impostas aos provedores de conexão e de aplicações de internet nos casos de descumprimento da legislação brasileira quanto à **coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais** e ao sigilo das comunicações privadas e dos registros. (STF, 2020, on-line, grifo nosso)

Ou seja, essa interpretação afasta, assim, qualquer estabelecimento de sanção em razão da inobservância de ordem judicial de disponibilização de conteúdo de comunicações, numa clara demonstração de que o espaço de privacidade, de intimidade e de liberdade dos usuários da Internet são os valores centrais da Lei 12.965/2014, que preza, acima de tudo, pela segurança jurídica no ambiente virtual.

Decorre, ainda, dessa interpretação a ideia de que a disponibilização de qualquer conteúdo de comunicações privadas somente pode ocorrer para fins de investigação criminal ou instrução processual penal, na forma estabelecida por lei, respeitado o disposto nos incisos II e III do art. 7º dessa legislação.

Esse mesmo entendimento foi defendido no julgamento da Arguição de Descumprimento de Preceito Fundamental (ADPF) 403, na qual se debateu os limites da decisão judicial a qual se refere o art. 7º, II, do Marco Civil da Internet, que restringe o direito à privacidade dos usuários de Internet ao permitir a violação e disponibilização do fluxo de comunicações em caso de ordem judicial.

Nessa decisão, o relator, Ministro Edson Fachin, afirmou que, a despeito de esse dispositivo configurar uma exceção à proteção da privacidade, é preciso ponderar se ela seria razoável o suficiente para justificar a sua aplicação. Segundo o Ministro, essa restrição somente seria cabível para casos mais graves, pois do contrário o ambiente virtual estaria sujeito a ingerências governamentais e à manipulação de dados, reduzindo a esfera de autonomia e determinação do indivíduo, ou seja, o seu direito à autodeterminação informacional.

Depreende-se da referida decisão, que "[...] na internet, a proteção de privacidade não é apenas proteção individual, mas garantia instrumental do direito à liberdade de expressão" (STF, 2020, on-line); por isso, considerando que a Constituição Federal outorga grande força a esse direito fundamental, é preciso lhe atribuir a máxima eficácia, mesmo diante de mudanças tecnológicas, o que se estende também aos dados pessoais, que são protegidos por mecanismos de anonimato e de criptografia, necessários ao combate da censura.

Nesse sentido, entende-se que, apesar de a criptografia trazer riscos à segurança pública, aumentando os custos para a realização de investigações criminais, o acesso a essa criptografia pelo Estado também representaria um risco à segurança de todos, reduzindo a proteção à integridade, ao sigilo, à confidencialidade, à autenticidade e à privacidade das mensagens transmitidas no ambiente virtual, não se justificando tal medida. Assim,

> É contraditório, portanto, que em nome da segurança pública deixe se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas. Não é isso, porém, o que ocorre. O risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional. (STF, 2020, on-line)

Diante disso, nas palavras do Ministro Edson Fachin, "[...] é inconstitucional proibir as pessoas de utilizarem a criptografia ponta-a-ponta, pois uma ordem como essa impacta desproporcionalmente as pessoas mais vulneráveis" (STF, 2020, on-line), sendo, portanto, possível o reconhecimento de um direito constitucional à criptografia e, consequentemente, aos direitos digitais, os quais, de acordo com esse relator, devem ser considerados direitos fundamentais.

Dessa forma, por entender que a sanção de suspensão prevista no inciso III do artigo 12 da Lei 12.965/2014 só deve ocorrer nos casos em que os provedores de aplicativos violarem os direitos de privacidade dos usuários e que a ordem judicial a que se refere o inciso II do artigo 7º dessa legislação, mesmo que para fins de investigação criminal ou instrução processual penal, não pode enfraquecer a proteção criptográfica e o direito à privacidade, além de outros direitos fundamentais, a Arguição de Descumprimento de Preceito Fundamental foi julgada procedente pelo relator desse processo, no sentido de declarar a inconstitucionalidade parcial sem redução de texto de ambas as normas, restando afastada qualquer interpretação que permita que ordem judicial "[...] exija acesso excepcional a conteúdo de mensagem criptografada ponta-a-ponta ou

que, por qualquer outro meio, enfraqueça a proteção criptográfica de aplicações da internet [...]" (STF, 2020, on-line).

Ou seja, depreende-se do teor dos votos analisados que o direito à privacidade dos usuários de Internet, mesmo quando conflita com o direito à segurança pública e à livre atuação do poder estatal no combate e na apuração de delitos, deve prevalecer, a fim de preservar a intimidade, a vida privada, a honra bem como o sigilo das comunicações, garantindo ainda a autodeterminação dos indivíduos, pressuposto também do direito à proteção de dados, matéria que, por sua vez, se fortaleceu com os avanços trazidos pelo Marco Civil da Internet.

Tais decisões significaram, assim, um marco significativo para o direito digital, agora reconhecido como um direito fundamental, e revelam as sucessivas mudanças na sociedade ocasionadas pelo impacto tecnológico. Consequência disso é a exigência por uma constante atualização do alcance dos direitos e garantias fundamentais pelo ente estatal, seja através de edições de novas legislações seja por intermédio da jurisprudência, dada a potencialização das violações que podem ser sofridas pelos indivíduos no ambiente virtual, principalmente em relação aos seus dados pessoais.

Afinal, boa parte da vivência das pessoas tem ocorrido dentro das redes, por meio de computadores e de celulares, onde se concentra atualmente parcela da nossa privacidade e intimidade. O acesso a fotos, vídeos e dados pessoais identificadores é facilmente obtido por intermédio não só das redes sociais como também de sítios eletrônicos diversos, a partir de cadastros, compras realizadas ou através de algoritmos, que registram as nossas "pegadas virtuais". Com isso, permite-se conhecer as preferências, orientação sexual e política, religião, profissão, dentre outras informações pessoais dos indivíduos que podem ser manipuladas com vários intuitos, inclusive fraudulentos.

Nesse sentido, o Marco Civil da Internet teve o condão não só de assegurar a prevalência do direito à privacidade (e direitos consectários) no ambiente virtual, conforme se depreende das decisões supramencionadas, como também serviu para fortalecer as bases para a construção de um direito autônomo à proteção de dados, que, por sua natureza e amplitude, além de demandar a edição de uma legislação específica, exigiu também do Poder Judiciário um tratamento a partir de uma perspectiva constitucional, como forma de tutelar não apenas a privacidade, mas também as liberdades e a personalidade do indivíduo.

4.2 O reconhecimento de um direito fundamental à proteção de dados pelo Supremo Tribunal Federal

A formulação do direito à proteção de dados como um direito independente traçou um longo caminho não só a nível brasileiro como também internacional. Conforme explanado no primeiro capítulo desse estudo, suas bases normativas e principiológicas têm origem no direito europeu, que contribuiu para desvencilhá-lo do direito à privacidade, com quem era tradicionalmente ligado, para configurá-lo como um direito fundamental autônomo, definindo-o como a prerrogativa que todo cidadão tem de dispor livremente de seus dados pessoais.

Esse poder de autodeterminação da pessoa de decidir sobre a disposição de seus dados remonta à decisão antológica da Corte Constitucional alemã, de 1983, que se tornou uma referência nessa área, ao assegurar não só o direito de participação e envolvimento do indivíduo no processo de coleta, armazenamento e transmissão dos seus dados, como também por relacioná-lo a um direito de personalidade, tendo em vista o foco concedido à proteção da pessoa em face dos riscos decorrentes da indevida manipulação de dados.

Na ocasião, a referida decisão, que reconheceu a Lei do Censo de 1982 como parcialmente inconstitucional por restringir o direito de liberdade do indivíduo no ato de fornecer informações pessoais à administração pública, afirmou:

> [...] A autodeterminação individual pressupõe - mesmo nas condições das modernas tecnologias de processamento da informação - que o indivíduo tenha liberdade para decidir sobre as ações a serem ou não realizadas, incluindo a possibilidade de realmente se comportar de acordo com essa decisão. Qualquer pessoa que não consiga ver com certeza suficiente quais informações são conhecidas por eles em certas áreas de seu ambiente social, e que não possa avaliar razoavelmente o conhecimento de possíveis parceiros de comunicação, pode ser significativamente inibida em sua liberdade de planejar ou decidir por sua própria iniciativa. O direito à autodeterminação informacional não seria compatível com uma ordem social e uma ordem jurídica que o possibilite, em que os cidadãos não possam mais saber quem sabe o que sobre eles, quando e em que ocasião (TCF, 1983, on-line).

Após isso, as legislações europeias que se seguiram consolidaram esse direito subjetivo à autodeterminação informativa, que posteriormente foi considerado um direito fundamental também pela Carta dos Direitos Fundamentais da União Europeia, sendo ainda incorporado ao texto de algumas Constituições não só de países europeus, mas também de outros continentes como um dos fundamentos do direito à proteção de dados.

Conforme aduz Danilo Doneda (2019, p. 169), citando Roppo (1984 p. 83):

> A influência da decisão alemã pode se fazer sentir em vários pontos. Um deles é a solidificação do entendimento segundo o qual a proteção de dados pessoais requer um

> embasamento constitucional direto – assim, respaldada como um direito fundamental, é possível a tutela da personalidade, mesmo numa área específica como a proteção de dados.

No Brasil, a Lei Geral de Proteção de Dados, fortemente influenciada pelo Regulamento Geral de Proteção de Dados (GDPR), também incluiu a autodeterminação informativa dentre os seus fundamentos e, a despeito de se tratar de uma legislação ordinária, ela trouxe uma carga normativa e principiológica que densificaram essa tendência internacional de uma constitucionalização do direito à proteção de dados no país.

Reflexo disso é a Proposta de Emenda à Constituição n° 17, de 2019, que inclui o direito à proteção de dados pessoais de forma expressa no texto constitucional, que até o presente momento não foi votada na Câmara dos Deputados, mas incluiu o tema na pauta de doutrinas pátrias, que já tendem a extrair a fundamentalidade desse direito de outras normas constitucionais explícitas, tais como o direito à privacidade (art. 5º, X), a proteção da dignidade da pessoa humana (art. 1º, III), dentre outros dispositivos. Como consequência, o Poder Judiciário passou também a se pronunciar, sendo chamado a produzir o Direito diante do constante cenário de risco que envolve o tratamento de dados.

No âmbito do Supremo Tribunal Federal, em 2015, ou seja, antes mesmo do advento da Lei 13.709/2018 e a PEC 17/2019, um debate sobre o direito do contribuinte de obter, através de *habeas data*, anotações, informações e dados a seu respeito constantes de sistema da Receita Federal sinalizou um primeiro passo para o reconhecimento judicial de um direito fundamental à proteção de dados no Brasil.

Nos autos do Recurso Extraordinário nº 673707 / MG, essa Corte entendeu que, apesar de esse remédio constitucional garantir o acesso a informações relativas à pessoa do impetrante que constam em registros ou bancos de dados de entidades governamentais ou de caráter público, o artigo 5º, inciso LXXII, da Constituição, na verdade, "não tem por objetivo negar a seu próprio titular o conhecimento das informações que a seu respeito estejam cadastradas junto às entidades depositárias" (STF, 2015, on-line). Esse dispositivo apenas busca restringir a divulgação dessas informações a outros órgãos, que não o detentor destas, ou a terceiros, devendo ser assegurado o acesso aos titulares de dados pessoais, pautando-se a Administração Pública pela publicidade e transparência de seus atos.

E por se tratar de dados pessoais pertencentes ao próprio requerente, esse Tribunal ainda entendeu que não haveria como prosperar qualquer tese de comprometimento da segurança da sociedade ou do Estado, devendo o *habeas data* servir como instrumento de tutela da autonomia

privada e da autodeterminação sobre os dados. É o que se depreende, por exemplo, do seguinte trecho do voto prolatado pelo Ministro Gilmar Mendes:

> É interessante que, quando se discutiu esse processo e a criação dessa garantia, olvidou-se de que já se discutia, em outras partes do mundo, a ideia numa perspectiva de direito material, que é o direito de autodeterminação sobre dados. No fundo, o nosso habeas data acabou tratando da temática processual, garantística processual, sem explicitar, pelo menos de maneira clara, o direito tutelado, que nós podemos identificar, claro, com os direitos de personalidade, a intimidade privada e assim por diante (STF, 2015, on-line).

Ainda nas palavras desse Ministro, por se tratar de um direito subjetivo material à proteção de dados do impetrante,

> Essa jurisprudência representa um passo fundamental na consolidação da tutela constitucional dos dados pessoais no Brasil e traz elementos relevantes para a compreensão de um direito material à proteção de dados, decorrente lógico e necessário da garantia processual do habeas data (STF, 2015, on-line).

De fato, esse julgado representou um grande avanço para a obtenção de uma visão constitucional do direito à proteção de dados no Brasil, a partir de uma percepção mais ampla da garantia processual *habeas data*, contribuindo não só para a construção desse direito material como também para a noção de um direito fundamental que servisse de resistência do cidadão a eventual arbítrio do Estado, o que posteriormente se concretizou em julgado recente também prolatado pelo Supremo Tribunal Federal, nos autos da Ação Direta de Inconstitucionalidade nº 6.387/DF proposta pelo Conselho Federal da Ordem dos Advogados do Brasil.

Essa ação, ajuizada juntamente com outras da mesma classe, ADI nº 6388, nº 6389, nº 6390 e nº 6393, por partidos políticos, teve como intuito a suspensão da aplicação da Medida Provisória nº 954/2020, que determinava que operadoras de telefonia compartilhassem dados pessoais de seus consumidores, incluindo nomes, números de telefone e endereços, com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), a fim de dar suporte à Pesquisa Nacional por Amostra de Domicílios (Pnad) Contínua durante a situação de emergência de saúde pública causada pelo coronavírus (covid19).

Tendo como suporte a Lei nº 13.979/2020, que dispõe sobre as medidas a serem adotadas pelo governo federal para enfrentamento da pandemia, essa Medida Provisória trazia o seguinte texto:

> Art. 1º Esta Medida Provisória dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras do Serviço Telefônico Fixo Comutado - STFC e do Serviço Móvel Pessoal - SMP com a Fundação Instituto Brasileiro de Geografia e Estatística - IBGE.

> Parágrafo único. O disposto nesta Medida Provisória se aplica durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020.
> Art. 2º As empresas de telecomunicação prestadoras do STFC e do SMP deverão **disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas.**
> **§ 1º Os dados de que trata o *caput* serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares.**
> § 2º Ato do Presidente da Fundação IBGE, ouvida a Agência Nacional de Telecomunicações, disporá, no prazo de três dias, contado da data de publicação desta Medida Provisória, sobre o procedimento para a disponibilização dos dados de que trata o *caput*.
> § 3º Os dados deverão ser disponibilizados no prazo de:
> I - sete dias, contado da data de publicação do ato de que trata o § 2º; e
> II - quatorze dias, contado da data da solicitação, para as solicitações subsequentes.
> **Art. 3º Os dados compartilhados:**
> **I - terão caráter sigiloso;**
> **II - serão usados exclusivamente para a finalidade prevista no § 1º do art. 2º; e**
> **III - não serão utilizados como objeto de certidão ou meio de prova em processo administrativo, fiscal ou judicial, nos termos do disposto na Lei nº 5.534, de 14 de novembro de 1968.**
> **§ 1º É vedado à Fundação IBGE disponibilizar os dados a que se refere o *caput* do art. 2º a quaisquer empresas públicas ou privadas ou a órgãos ou entidades da administração pública direta ou indireta de quaisquer dos entes federativos.**
> § 2º A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no *caput* do art. 2º foram utilizados e divulgará **relatório de impacto à proteção de dados pessoais, nos termos do disposto na Lei nº 13.709, de 14 de agosto de 2018.**
> Art. 4º Superada a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), nos termos do disposto na Lei nº 13.979, de 2020, as informações compartilhadas na forma prevista no *caput* do art. 2º ou no art. 3º serão eliminadas das bases de dados da Fundação IBGE.
> Parágrafo único. Na hipótese de necessidade de conclusão de produção estatística oficial, a Fundação IBGE poderá utilizar os dados pelo prazo de trinta dias, contado do fim da situação de emergência de saúde pública de importância internacional.
> Art. 5º Esta Medida Provisória entra em vigor na data de sua publicação.
> Brasília, 17 de abril de 2020; 199º da Independência e 132º da República. (grifo nosso) (BRASIL, 2020)

Na ADI nº 6.387/DF, o autor da ação pediu a procedência do pedido de declaração de inconstitucionalidade da mencionada Medida Provisória em sua integralidade, por entender que ela violava normas constitucionais que dispõem sobre a dignidade da pessoa humana, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o sigilo dos dados e a autodeterminação informativa, além de não observar o constante do artigo 62, *caput*, da Constituição Federal, uma vez que não estariam presentes os requisitos da urgência e da relevância material que autorizam a edição de medida provisória.

Ademais, alegou o autor que não era possível depreender da MP 954/2020 a relevância da pesquisa estatística que pudesse justificar o referido compartilhamento de dados, de que

forma seria feito e como isso seria útil no enfrentamento da crise sanitária. Não teria ainda, segundo o autor, sido esclarecido a finalidade e a adequação do compartilhamento de dados, uma vez que o próprio IBGE já tinha comunicado o adiamento do Censo Demográfico para o ano de 2021[78]. Por fim, o autor requereu o reconhecimento de um direito fundamental à proteção de dados e à autodeterminação informativa.

Em abril de 2020, a relatora do processo, Ministra Rosa Weber, deferiu a medida cautelar pleiteada nos autos, no sentido de suspender a eficácia da MP nº 954/2020, determinando ainda que o IBGE se abstivesse de requerer a disponibilização dos dados da qual ela tratava, por entender que esse instrumento normativo não atendia às exigências do texto constitucional referentes à proteção de direitos fundamentais dos brasileiros. Poderia, assim, esse compartilhamento de dados trazer danos irreparáveis à intimidade e ao sigilo da vida privada de milhares de consumidores das operadoras de telefonia locais.

Essa medida cautelar foi referendada em maio de 2020, ocasião em que a citada relatora ainda afirmou que, após tomar conhecimento de que o IBGE já havia iniciado, naquela data, a PNAD Contínua com uma amostra de 211 mil domicílios que já tinham participado dessa pesquisa no primeiro trimestre de 2019, essa fundação pública só evidenciava a desnecessidade de compartilhamento de milhões de números de telefone de brasileiros para a finalidade invocada na MP nº 954/2020, não justificando esse excesso diante dos riscos inerentes à manipulação desses dados.

Assim, de acordo com a relatora, esse ato não delimitava “o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente, não esclarece a necessidade de disponibilização dos dados, nem como serão efetivamente utilizados" (STF, 2020, on-line).

Segundo a Ministra Rosa Weber, esse instrumento normativo ainda se mostrou desproporcional por prever a conservação dos dados pessoais, pelo ente público, por tempo manifestamente excedente ao estritamente necessário para a pesquisa estatística e por não trazer qualquer previsão sobre a anonimização ou pseudonimização dos dados coletados, a fim de evitar a identificação dos titulares dos dados, não assegurando, portanto, um tratamento seguro.

Por entender que a Constituição Federal de 1988 consagrou, de forma específica, a intimidade, a vida privada e o sigilo de dados, sendo este último um instrumento democrático

[78] Registra-se que, na mesma data de publicação da MP nº 954/2020, o governo federal editou a Instrução Normativa nº 2/2020, que estabelece os procedimentos para disponibilização de dados de empresas de telecomunicações prestadoras de serviço telefônico fixo ou móvel ao IBGE, “para fins de suporte à produção de estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19)”. (BRASIL, 2020)

que refletia uma limitação do exercício do poder do Estado, em seu voto, o Ministro Alexandre de Moraes ainda afirmou que estes se tratam de "comandos proibitórios expressos dirigidos ao Estado não violar a intimidade, a vida privada e o sigilo de dados" (STF, 2020, on-line). Ademais, segundo ele, não seria possível, nesse caso, a relativização desse sigilo de dados, uma vez que não estariam configuradas a adequação, a razoabilidade e a proporcionalidade do ato normativo em questão, o que poderia levar a arbitrariedades em relação aos direitos e garantias individuais tutelados constitucionalmente em caso de divulgação dos dados coletados. Afinal,

> Os direitos e garantias individuais não podem, por óbvio, ser utilizados como verdadeiro escudo protetivo da prática de atividade ilícitas, tampouco como argumento para afastar ou diminuir a responsabilidade civil, tributária ou penal por atos criminosos, sob pena também de desrespeito ao verdadeiro Estado de Direito. (STF, 2020, on-line)

O Ministro Edson Fachin, por sua vez, ao mesmo tempo em que reconheceu o papel do IBGE e a sua importância para a formulação de políticas públicas e para o exercício da cidadania e da democracia brasileira, afirmou que "nem a excepcionalidade da crise vivida, nem a valorosa tarefa de produzir estudos estatísticos justifica a violação dos direitos fundamentais dos usuários dos serviços de telefonia". De acordo com o seu voto,

> A Medida Provisória nº 954/2020 intervém fortemente na esfera nuclear da configuração da vida privada. Uma intervenção dessa natureza só seria possível com o reforço das garantias de natureza procedimental. Apenas um incremento do conjunto de filtros e salvaguardas relativos aos dados dos usuários dos serviços de telefonia poderia, a priori, justificar tal ingerência (STF, 2020, on-line).

Registra-se ainda importante colocação do Ministro Luís Roberto Barroso, ao expor sua preocupação com os riscos e as ameaças que envolvem o tratamento de dados, que podem ser utilizados para uso indevido, "inclusive e sobretudo para fins políticos" (STF, 2020, on-line). Conforme esse Ministro,

> A questão jurídica que está em jogo, como se percebe nitidamente, é a ponderação entre dois valores importantes. De um lado, a estatística, que não é um valor em si, mas é um instrumento, uma ferramenta indispensável no mundo contemporâneo para que se desenhem políticas públicas adequadas para atender as necessidades da população. [...]. No outro prato dessa balança, estão os direitos constitucionais elencados no art. 5º da Constituição, X e XII, notadamente o direito à intimidade e à vida privada, genericamente identificados com o direito de privacidade, que é o direito que toda pessoa tem de ter uma esfera da sua vida que não seja acessível, quer ao Estado, quer a outras pessoas, salvo, eventualmente, por vontade própria (STF, 2020, on-line).

Tais colocações reforçam, portanto, a tensão existente entre a relevância dos dados pessoais atualmente e os riscos provenientes do seu uso indevido, causando ainda maior

preocupação, nesse caso, a possibilidade de a coleta destes se dar a partir de um ato normativo que não deixa clara nem a sua finalidade nem a certeza de segurança no tratamento desses dados através de métodos eficientes, se mostrando vaga a MP nº 954/2020 nesse sentido.

Isso porque, sem essa segurança, esses dados estariam à mercê de acessos desautorizados, vazamentos acidentais, além de cruzamentos com outras informações compartilhadas por demais entidades que tornariam essa operação potencialmente perigosa, não podendo ser relevado ainda o risco de formação de perfil dos usuários de serviços de telefonia móvel e fixa a partir da coleta de seus nomes, endereços e telefones, como bem lembra o Ministro Gilmar Mendes:

> A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e de empresas utilizem algoritmos e ferramentas de data analytics, que promovem classificações e esteriotipações discriminatórias de grupos sociais para a tomada de decisões estratégias para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham (STF, 2020, on-line).

Por isso, afirmou o Ministro Luiz Fux, após criticar também o fato de a MP nº 954/2020 ter previsto a realização de relatório de impacto à proteção de dados pessoais somente após o compartilhamento e tratamento dos dados dos cidadãos, quando esse documento deveria ser confeccionado antes da coleta, a fim de garantir a transparência da operação:

> As leis que tratam da coleta e processamento de dados devem atender a propósitos legítimos, específicos, explícitos e informados, limitar a coleta ao mínimo necessário para a realização de suas finalidades normativas – o que não ocorre com essa medida provisória -, prever medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais e prevenir a ocorrência de danos. Prevenir a ocorrência de danos. Então, o minimalismo é exatamente o que recomenda que se utilize nessa medida provisória que determinou esse compartilhamento de tantos dados (STF, 2020, on-line).

É importante frisar ainda que, na época do julgamento da ADI nº 6.387/DF, em maio de 2020, a Lei Geral de Proteção de Dados - LGPD (Lei 13.709/18) ainda estava em *vacatio legis*, o que não impediu que essa decisão fizesse claras referências aos princípios previstos nesta legislação, quais sejam a finalidade, a adequação, a necessidade, a segurança e a prevenção nas atividades de tratamento de dados pessoais que seriam realizadas pelo IBGE. Essa decisão mostrou também a preocupação quanto à ausência de uma autoridade administrativa para acompanhar e fiscalizar essa operação, no caso a ANPD, o que agravava mais ainda as imprecisões e deficiências da MP nº 954/2020.

É possível extrair ainda dessa decisão a forte preocupação com a proteção do indivíduo através da tutela da sua privacidade e da sua intimidade, direitos estes que, embora não sejam absolutos, não admitiam, no caso concreto, quaisquer restrições diante dos eventuais riscos que envolviam a aplicação dessa Medida Provisória. É o que se depreende das palavras do Ministro Ricardo Lewandowski em seu voto:

> [...] Sempre que configurada a verticalidade de tais relações jurídicas (Estado x cidadãos), a observância de, absolutamente, todos os direitos e garantias constitucionais contra o arbítrio estatal ganha ainda mais importância, independentemente do grave momento de pandemia pelo qual o País.
> [...]
> É preciso ficar claro, portanto, que não se está a falar de informações insignificantes, mas da chave de acesso a dados de milhões de pessoas, com alto valor para execução de políticas públicas, é verdade, mas também com provável risco de adoção de expedientes, por vezes, dissimulados, obscuros, que possam causar desassossego na vida diária do indivíduo (STF, 2020, on-line).

Esse Ministro defendeu também que a MP nº 954/2020 fere, "por consequência, os princípios da ordem econômica, da defesa do consumidor, do livre desenvolvimento da personalidade e da dignidade, bem como o exercício da cidadania quanto às pessoas naturais" (STF, 2020, on-line), sendo, portanto, possível concluir que, quando se trata de operações relacionadas a dados pessoais, inevitavelmente há uma vulnerabilidade de todo o sistema de proteção de garantias individuais.

Por tais motivos, a decisão prolatada nos autos da ADI nº 6.387/DF foi considerada paradigmática no direito pátrio, pois, pela primeira vez, a proteção de dados pessoais e a autodeterminação informativa foram reconhecidas como direitos fundamentais, em situação semelhante a que ocorreu com a Lei do Censo de 1982 e a sentença da Corte Constitucional alemã, numa clara demonstração de que o catálogo de direitos fundamentais tem se adaptado às transformações tecnológicas.

Inclusive, nas palavras do Ministro Gilmar Mendes, seria um dever do Supremo Tribunal Federal "aprofundar a identificação, na ordem constitucional brasileira, de um direito fundamental à proteção de dados pessoais, a fim de estabelecer de forma clara o âmbito de proteção e os limites constitucionais à intervenção estatal sobre essa garantia individual" (STF, 2020, on-line). Segundo ele:

> A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas.
> [...]

> Desse modo, a afirmação da força normativa do direito fundamental à proteção de dados pessoais decorre da necessidade indissociável de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional nas sociedades contemporâneas (STF, 2020, on-line).

Dessa forma, depreende-se do entendimento dessa Corte que esse direito fundamental à proteção de dados deve ser considerado autônomo, que demanda tutela jurídica e âmbito de incidência específicos. Isso porque, apesar de ser extraído da garantia da inviolabilidade da intimidade e da vida privada e do princípio da dignidade da pessoa humana previsto constitucionalmente, tais direitos acabam por se diferenciar da proteção de dados, que tem objeto de proteção distinto.

O fato, assim, de ser considerado um direito fundamental, cuja lógica e essência são retiradas de uma leitura sistemática das garantias constitucionais, fez com que o direito à proteção dos dados dos usuários de telefonia fixa e móvel, no caso concreto, se sobrepujasse ao interesse público em questão, levando à suspensão da eficácia da Medida Provisória nº 954/2020 pelo Supremo Tribunal Federal, conforme decisão assim ementada e publicada em 12 de novembro de 2020, *in verbis:*

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. **Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos**. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. 3. O Regulamento Sanitário Internacional (RSI 2005) adotado no âmbito da Organização Mundial de Saúde exige, quando essencial o tratamento de dados pessoais para a avaliação e o manejo de um risco para a saúde pública, a garantia de que os dados pessoais manipulados sejam "adequados, relevantes e não excessivos em relação a esse propósito" e "conservados apenas pelo tempo necessário." (artigo 45, § 2º, alíneas "b" e "d"). 4. **Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia**. 5. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação

> quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros. 7. **Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada**. 8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020. 9. **O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição**. 10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel. 11. Medida cautelar referendada. (STF, 2020, on-line, grifo nosso)

É possível, portanto, concluir da referida decisão que, no contexto da proteção de dados, a tutela do indivíduo necessariamente demanda uma compreensão integrada do texto constitucional, que perpassa pelo direito à intimidade, à vida privada e ao sigilo de dados, culminando na dignidade da pessoa humana e no livre desenvolvimento da personalidade, motivo pelo qual essa Corte decidiu pelo reconhecimento de um direito fundamental à proteção de dados, seguindo linha de entendimento já defendida por algumas doutrinas pátrias, conforme exposto ao longo dessa dissertação.

Inclusive, nesse sentido, já afirmava Danilo Doneda (2010, p. 49):

> O reconhecimento da proteção de dados como um direito autônomo e fundamental, portanto, não deriva de uma dicção explícita e literal, infere-se da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade pessoal humana, juntamente com a proteção da intimidade e da vida privada.

De qualquer forma, esse julgado representou um importante passo na área da proteção de dados no Brasil, contribuindo para o amadurecimento da matéria e servindo como ponto de partida para a análise de outros casos que sobrevieram a essa decisão, tal como ocorreu com a Arguição de Descumprimento de Preceito Fundamental nº 695 e com as Ações Diretas de

Inconstitucionalidade nº 6529 e nº 6561 julgadas recentemente pelo STF, demonstrando, mais uma vez, a atualidade do tema debatido nesta dissertação.

Na ADPF nº 695, por exemplo, que teve decisão liminar publicada em junho de 2020, o Partido Socialista Brasileiro (PSB), requereu que fosse reconhecida e sanada grave lesão a preceitos fundamentais praticada pelo Poder Público, após a Agência Brasileira de Inteligência (ABIN) ter solicitado ao Serviço Federal de processamento de Dados (SERPRO) o compartilhamento de dados de mais de 76 milhões de brasileiros que possuem a Carteira Nacional de Habilitação, coletados do Departamento Nacional de Trânsito (DENATRAN).

Ambas as instituições, ABIN e SERPRO, confirmaram a prática de tal conduta, com fundamento no Decreto 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal, tendo o DENATRAN, na época, emitido em favor da ABIN o Termo de Autorização nº 07/2020, que deferia o pedido de compartilhamento feito por este último, na Portaria nº 15/2016. A constitucionalidade de tais atos do Poder Público seriam, assim, o objeto de impugnação nesta ação.

Em seu voto, o Ministro Relator Gilmar Mendes lembrou não ser possível analisar a alegada constitucionalidade sem antes fazer um exame da legislação aplicável ao tratamento de dados pessoais pelo Poder Público, em que pese as legislações infraconstitucionais não sejam um parâmetro de controle de constitucionalidade de atos da Administração Pública (STF, 2020, on-line).

Remontando à paradigmática decisão prolatada pelo Tribunal Constitucional Alemão, em 1983, que declarou a inconstitucionalidade da chamada Lei do Censo alemã e reconheceu o direito à autodeterminação informacional, esse Ministro afirmou que o Supremo Tribunal Federal tem proporcionado, através de sua jurisprudência, tal como ocorreu com a Corte alemã, a abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados, citando, dentre outros julgados, a decisão prolatada na ADI 6387 (acima explanada), motivo pelo qual entendeu esse Relator que o caso em questão deveria também ser examinado sob essa ótica.

Dessa forma, a despeito de atos públicos ora impugnados preverem o dever de sigilo quanto ao uso das informações referentes aos dados disponibilizados, o Ministro afirmou que eles refletem “uma concepção jurídica ultrapassada que ombreia o direito à privacidade ao direito fundamental ao sigilo” (STF, 2020, on-line), pois não trazem garantias suficientes ao cidadão no que se refere ao controle sobre os seus dados. Esses atos não teriam resguardado, ainda, o direito fundamental à proteção de dados pessoais, a despeito do argumento utilizado

pela União no sentido de que o compartilhamento dos dados objeto do Termo de Autorização 7/2020, emitido pelo DENATRAN, seria limitado a dados não sensíveis.

É o que se depreende do seguinte trecho, *in verbis:*

> Diferentemente do que ocorre com o direito fundamental ao sigilo, a **dimensão subjetiva** do Direito Fundamental à Proteção de Dados Pessoais impõe que o legislador e o Poder Público de modo geral assumam o **ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional**.
> [...]
> Assim, no caso em tela, o que está em jogo não é apenas o nível de segurança da informação objeto do compartilhamento entre DENATRAN e ABIN, mas sim **a existência de mecanismos adequados de controle das finalidades desse compartilhamento.** Essa nova abordagem jurídica do direito fundamental à proteção de dados, nesse aspecto, engloba uma proteção abrangente, que desloca o eixo da proteção do conteúdo dos dados para as possibilidades e finalidades do seu processamento (STF, 2020, on-line, grifo do autor)

Em seu voto, o Ministro Gilmar Mendes reconhece, ainda, que o tratamento de dados é uma "importantíssima ferramenta para o desenho, implementação e monitoramento e políticas e de serviços públicos essenciais" (STF, 2020, on-line), que ainda exterioriza uma gestão pública eficiente. No entanto, ele pontua que

> [...]a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais.
> [...]
> A consciência de que os governos devem tratar o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais, é corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais (STF, 2020, on-line).

Por essa razão, depreende-se dessa decisão que o processamento dos dados dos cidadãos pelo Poder Público deve observar limitações normativas, a exemplo do que já ocorre em outros países, como forma de proteger a garantia da autodeterminação informativa, pois, "mesmo que se entenda que o direito fundamental à proteção de dados pessoais não é absoluto, é inequívoco que se deve buscar uma harmonização dos interesses do Estado tutelados constitucionalmente com os imperativos de proteção de garantias individuais" (STF, 2020, on-line).

Ademais, ao analisar os fundamentos legais trazidos pela União, o Relator da ADPF nº 695 lembrou que, atualmente, o tratamento de dados pelo Poder Público é regido pela Lei Geral de Proteção de Dados, pelo Decreto 10.046/2019, que instituiu o chamado Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, além do Decreto 9.929/2019, que criou o Sistema Nacional de Informações de Registro Civil – SIRC e do Decreto 10.046/2019, que

instituiu o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, este último apontado como fundamento legal para os atos do Poder Público impugnado nesta ação e a quem o Ministro teceu duras críticas:

> Embora o Decreto 10.046/2019 faça uma referência isolada à LGPD, verifica-se que, na realidade, ele afasta-se radicalmente da lógica de afirmação do princípio da finalidade consagrado na Lei Geral de Proteção de Dados. **O decreto, em vez disso, tende a reduzir – ou até mesmo eliminar – as barreiras ao livre fluxo de compartilhamento de dados pessoais na Administração Pública**. Para isso, ele explicitamente dispensa a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades públicas (art. 5º) (STF, 2020, on-line, grifo do autor).

Da mesma forma, rechaçou os argumentos utilizados pela União, no sentido de que o compartilhamento dos dados em questão estaria também inserido no âmbito da atividade de inteligência da ABIN, estabelecida no art. 5º da Lei 9.883/1999, afirmando não existir "uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no Poder Público, inclusive para realização das atividades de inteligência nacional" (STF, 2020, on-line), motivo pelo qual

> [...] convênios e acordos de compartilhamento baseados única e exclusivamente nas disposições do Decreto 10.046/2020 parecem afigurar-se potencialmente lesivos às garantias individuais discutidas nesta ADPF, a depender, é claro, das condições de compartilhamento e dos riscos envolvidos (STF, 2020, on-line).

Nos atos públicos impugnados, não estariam presentes ainda os requisitos da necessidade, da finalidade e da proporcionalidade em sentido estrito do compartilhamento de dados desejado, este último consistente na análise se "o interesse público atinente a esse processamento é superior ao interesse público da coletividade envolvido na vulneração da proteção dos dados pessoais" (STF, 2020, on-line). Por isso

> [...] no caso concreto, há significativa e densa verossimilhança nas alegações do autor, no sentido de que o ato do Poder Público trazido a exame por esta Suprema Corte (i) tem o potencial de violar os preceitos fundamentais da proteção da privacidade, da proteção de dados e da autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII, da CF/88); (ii) não possui base normativa que eventualmente lhe ampare – o que poderia em tese lhe emprestar legitimidade; e (iii) tampouco mostra-se proporcional ante as suas finalidades (STF, 2020, on-line).

Representou, com isso, a referida decisão, mais uma importante contribuição da jurisprudência do Supremo Tribunal Federal para o reconhecimento da proteção de dados enquanto direito fundamental, que se aplica também ao tratamento e ao compartilhamento de dados pelo Poder Público, um reflexo da abertura constitucional concedida à matéria, que impõe

a necessidade de compatibilização desse direito com outras importantes garantias constitucionais, conforme se depreende do seguinte trecho desse julgado:

> Como amplamente analisado nesta decisão, **o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea** (STF, 2020, on-line, grifo do autor)**.**

Tem-se, assim, que, em casos de compartilhamento de dados pela Administração Pública, deve ser dispensado o mesmo tratamento aos setores privados, observando-se, em cada contexto, a finalidade, a necessidade e a proporcionalidade desse ato, com vistas a evitar o risco de violação de preceitos fundamentais e proteger as garantias individuais de eventuais abusos estatais.

Já na ADI nº 6529, a Rede Sustentabilidade e o Partido Socialista Brasileiro pleitearam medida cautelar com vistas a reconhecer a inconstitucionalidade do parágrafo único do art. 4º da Lei nº 9.883/1999, que instituiu o Sistema Brasileiro de Inteligência, criando a Agência Brasileira de Inteligência (ABIN), e traz a seguinte redação:

> Art. 4º À ABIN, além do que lhe prescreve o artigo anterior, compete:
> [...]
> Parágrafo único. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais (BRASIL, 1999).

Requereram, ainda, os autores o afastamento da hipótese de aplicação do § 1º do artigo 2º da Lei nº 9.883/99, e do *caput* do artigo 9º-A desse diploma legal, que estatuem, respectivamente:

> Art. 2º. Os órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do Presidente da República.
> § 1º O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do Poder Executivo, bem como pela salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados.
> [...]
> Art. 9º A. Quaisquer informações ou documentos sobre as atividades e assuntos de inteligência produzidos, em curso ou sob a custódia da ABIN somente poderão ser fornecidos, às autoridades que tenham competência legal para solicitá-los, pelo Chefe do Gabinete de Segurança Institucional da Presidência da República, observado o respectivo grau de sigilo conferido com base na legislação em vigor, excluídos aqueles

> cujo sigilo seja imprescindível à segurança da sociedade e do Estado (BRASIL, 1999).

Tais pedidos, que conduziam, por consequência, ao afastamento do § 3º do art. 1º[79], da Estrutura Regimental da Agência Brasileira de Inteligência, constante do Decreto n. 10.445/2020, se fundamentavam, segundo os autores, no aumento do poder requisitório de informações pela Abin, à revelia de direitos fundamentais do cidadão, como a privacidade, a intimidade, o sigilo protegido pela cláusula de reserva de jurisdição, dentre outros.

Para os autores, tais dispositivos permitem que dados de investigações sigilosas, sigilo fiscal, relatórios do COAF, dados de sigilo telefônico, além de outras informações sensíveis e sigilosas sejam compartilhadas dentro do Sistema Brasileiro de Inteligência sem a devida motivação e com possibilidades reais de desvirtuamento da finalidade da Abin, tornando vulneráveis direitos fundamentais básicos dos cidadãos.

Mas em decisão que tratou da medida cautelar pleiteada, a Ministra relatora Cármen Lúcia afirmou que, a despeito das alegações dos autores, não se vislumbrava, no quadro normativo questionado, qualquer desvio de finalidade ou abuso de direito, tendo o fornecimento e compartilhamento de dados, pelos órgãos componentes do Sistema Brasileiro de Inteligência à ABIN, como único motivo legalmente admissível a defesa das instituições e dos interesses nacionais" (STF, 2020, on-line), não sendo válida qualquer outra interpretação.

De acordo com esse julgado, caracterizaria ato ilícito e, consequentemente, ato atentatório a direitos fundamentais dos cidadãos caso o fornecimento dessas informações viesse a atender fins privados ou pessoais, o que configuraria uma espionagem ilegal. Assim, "comprovado o descumprimento dos princípios constitucionais há de ser declarado ilegítimo pelo Poder Judiciário, inclusive em seu desempenho de controle abstrato de constitucionalidade da norma" (STF, 2020, on-line).

Dessa forma, afirmou a Ministra Cármen Lúcia que "não é o conteúdo da norma legal erigida em objeto da presente ação que é tida como possibilitadora do desvio de finalidade, mas a sua implementação normativa infralegal que pode fazer vingar a semente do vício acima mencionado" (STF, 2020, on-line). Ela ainda completou:

---

[79] Afirma essa norma: "Art. 1º. A Agência Brasileira de Inteligência - Abin, órgão integrante do Gabinete de Segurança Institucional da Presidência da República, criada pela Lei nº 9.883, de 7 de dezembro de 1999, é órgão central do Sistema Brasileiro de Inteligência e tem por competência planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do País, obedecidas a política e as diretrizes estabelecidas em legislação específica. [...] § 3º Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à Abin, sempre que solicitados, nos termos do disposto no Decreto nº 4.376, de 13 de setembro de 2002, e na legislação correlata, para fins de integração, dados e conhecimentos específicos relacionados à defesa das instituições e dos interesses nacionais" (BRASIL, 2020).

> O parágrafo único do art. 4º da Lei nº 9.883/99, nos seus expressos termos e, como antes acentuado, em seus mais de vinte anos de vigência, compatibiliza-se com a Constituição da República de 1988 com a interpretação que lhe vem dos próprios termos e que deixam resguardadas competências dos demais órgãos dos Poderes da República e, principalmente, dos direitos individuais intocáveis dos indivíduos.
> [...]
> O seu descumprimento parece nem decorrer propriamente de má interpretação, mas de negativa a sua aplicação, pois em seus termos se dispõe que o fornecimento de dados e conhecimentos específicos dos órgãos componentes do Sistema Brasileiro de Inteligência com a ABIN somente é possível quando comprovado o interesse público, vedada, portanto, qualquer destinação que atenda a interesse particular ou privado. (STF, 2020, on-line).

Chama atenção, no entanto, nesse julgado, as palavras do Ministro Gilmar Mendes, que, em seu voto, ressaltou que o tema debatido se relaciona com o direito à proteção de dados, referindo-se a este como um direito fundamental:

> O parâmetro de controle invocado nesta ADI está relacionado à afirmação do direito à proteção de dados pessoais enquanto categoria autônoma de direito fundamental na ordem constitucional brasileira, especialmente na forma de uma projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, consagrado no art. 5º, inciso X, da CF (STF, 2020, on-line).

Reiterando o entendimento já esposado nos autos da ADI nº 6387, esse Ministro lembrou que o direito fundamental à proteção de dados guarda uma dimensão objetiva, que "impõe ao legislador um verdadeiro dever de proteção (*Schutzpflicht*) do direito à autodeterminação informacional" (STF, 2020, on-line), bem como uma dimensão subjetiva, que "impõe que o legislador e o Poder Público de modo geral assumam o ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional" (STF, 2020, on-line). Nesse aspecto

> A autodeterminação do titular sobre os dados deve ser sempre a regra, somente afastável de maneira excepcional. A justificativa constitucional da intervenção deve ser traduzida na identificação da finalidade e no estabelecimento de limites ao tratamento de dados em padrão suficientemente específico, preciso e claro para cada área (STF, 2020, on-line).

Diante disso, é possível afirmar que esse direito de autodeterminação não protege especificamente os dados, mas a pessoa em si, tendo em vista os riscos provenientes de um tratamento de dados indevido, sendo a partir deste prisma, segundo o Ministro Gilmar Mendes, que deve ser examinada a constitucionalidade dos dispositivos impugnados da Lei 9.883, de 1999 (STF, 2020, on-line).

Assim, no que tange ao processamento de dados pessoais pelo Poder Público, deve a Administração Pública sempre compatibilizar seus interesses com a defesa de garantias individuais, atendendo aos valores constitucionais da eficiência da Administração Pública, mas obedecendo também a finalidade legítima e a proporcionalidade compatível com esse ato, o que inclui a execução de atividades de inteligência. Por esse motivo, segundo o Ministro Gilmar Mendes, "o art. 4º da lei buscou, na medida do possível, regulamentar o planejamento e a execução de atividades sigilosas na produção de conhecimentos destinados ao assessoramento da Presidência da República" (STF, 2020, on-line). No entanto, apesar disso, ele pontua:

> Verifica-se que o art. 4º, parágrafo único, da lei, ao contemplar a análise de dados como etapa essencial das atividades de inteligência, esclareceu a possibilidade – e não necessariamente a obrigatoriedade – de compartilhamento de dados entre os órgãos componentes do Sistema.
> Essa simples previsão legal, porém, apesar de ser necessária, não é em si suficiente para legitimar todo e qualquer procedimento de compartilhamento e requisição de dados, uma vez inafastável a observância das garantias institucionais de cunho constitucional, sobretudo naquilo que diz respeito ao direito ao sigilo ou a reserva de jurisdição (STF, 2020, on-line).

Entendeu, dessa forma, esse Ministro que, por não ser possível, da leitura da norma, "conhecer antecipadamente a natureza dos dados compartilhados tampouco os parâmetros objeto do compartilhamento no âmbito do Sistema Brasileiro de Inteligência" (STF, 2020, on-line), faltou, por parte do legislador, além de explanar a finalidade de tais atos, "adotar salvaguardas mais expressas que garantissem minimamente o controle das condicionantes das solicitações de requisições de informações no âmbito dos órgãos componentes do SBIN" (STF, 2020, on-line), o que o levou a concluir que

> [...] no caso concreto, há alguma verossimilhança nas alegações da autora, no sentido de que **o ato normativo trazido a exame desta Suprema Corte – justamente por contemplar aplicações múltiplas e genéricas – tem o potencial de violar os direitos fundamentais da proteção da privacidade, da proteção de dados e da autodeterminação informativa dos cidadãos brasileiros** (art. 5º, incisos X e XII, da CF/88), e tampouco mostra-se proporcional ante as suas finalidades (STF, 2020, on-line) (grifo nosso).

Por tais motivos, tendo em vista que "a autorização para o levantamento do sigilo dos dados retrata uma excepcionalidade do direito fundamental de proteção à intimidade e à vida privada (CF/88, art. 5º, X), que é a regra na ordem constitucional pátria" (STF, 2020, on-line), e que deve o Poder Público atender ao princípio da proporcionalidade, da devida fundamentação das decisões e da reserva constitucional de jurisdição ao restringir o domínio do indivíduo sobre suas informações, essa Corte Suprema decidiu por deferir parcialmente a medida cautelar

requerida pelos autores, nos autos da ADI nº 6529, no sentido de dar interpretação conforme a Constituição ao parágrafo único do art. 4º da Lei nº 9.883/99, em decisão publicada em outubro de 2020, que ficou assim ementada:

> DIREITO CONSTITUCIONAL. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/99. INTERESSE PÚBLICO FORMALMENTE DEMONSTRADO COMO ÚNICO ELEMENTO LEGITIMADOR DO DESEMPENHO ADMINISTRATIVO. VEDAÇÃO AO ABUSO DE DIREITO E AO DESVIO DE FINALIDADE. OBRIGATORIEDADE DE MOTIVAÇÃO DO ATO ADMINISTRATIVO QUE SOLICITA DADOS DE INTELIGÊNCIA AOS ÓRGÃOS DO SISTEMA BRASILEIRO DE INTELIGÊNCIA. NECESSÁRIA OBSERVÂNCIA DA CLÁUSULA DE RESERVA DE JURISDIÇÃO. DEFERIMENTO PARCIAL DA MEDIDA CAUTELAR PARA DAR INTERPRETAÇÃO CONFORME AO PARÁGRAFO ÚNICO DO ART. 4º DA LEI N. 9.883/99. 1. Para se concluir válido o texto legal e dar-se integral cumprimento ao comando normativo infralegal pelo Poder Executivo há de adotar-se como única interpretação e aplicação juridicamente legítima – como é óbvio – aquela que conforma a norma à Constituição da República. É imprescindível vinculem-se os dados a serem fornecidos ao interesse público objetivamente comprovado e com motivação específica. 2. Todo fornecimento de informação entre órgãos que não cumpra os rigores formais do direito nem atenda estritamente ao interesse público, rotulado legalmente como defesa das instituições e do interesse nacional, configura abuso do direito, contrariando a finalidade legítima posta na norma legal. 3. Práticas de atos à margem ou diversos do interesse público, especificado em cada categoria jurídica, devem ser afastadas pelo Poder Judiciário, quando comprovado o desvio de finalidade no cometimento. 4. A ausência de motivação expressa impede o exame da legitimidade de atos da Administração Pública, incluídos aqueles relativos às atividades de inteligência, pelo que a motivação é imprescindível. 5. Mesmo nos casos de prática de atos motivados pelo interesse público, não é possível que os órgãos componentes do Sistema Brasileiro de Inteligência forneçam à ABIN dados que importem em quebra do sigilo telefônico ou de dados, por ser essa competência conferida ao Poder Judiciário, nos termos constitucionalmente previstos. 6. Medida cautelar parcialmente deferida para dar interpretação conforme ao parágrafo único do art. 4º da Lei nº 9.883/99 estabelecendo-se que: a) os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à ABIN quando comprovado o interesse público da medida, afastada qualquer possibilidade desses dados atenderem interesses pessoais ou privados; b) toda e qualquer solicitação de dados deverá ser devidamente motivada para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal, em razão daquela limitação, decorrente do necessário respeito aos direitos fundamentais; d) nas hipóteses cabíveis de fornecimento de informações e dados à ABIN é imprescindível procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização, em caso de eventual omissão desvio ou abuso. (STF - ADI 6529 MC, Relator(a): CÁRMEN LÚCIA, Tribunal Pleno, julgado em 13/08/2020, PROCESSO ELETRÔNICO DJe-249, DIVULG 14-10-2020 PUBLIC 15-10-2020)

Em mais uma decisão também recente, nos autos da ADI nº 6561, datada de outubro de 2020, o Supremo Tribunal Federal foi instado a analisar a inconstitucionalidade formal e

material da Lei 3.528, de 12 de agosto de 2019, do Estado do Tocantins, que criou o Cadastro Estadual de Usuários e Dependentes de Drogas.

Infere-se dessa decisão que essa lei previu a criação de uma lista de usuários e de dependentes de drogas pela Secretaria de Segurança Pública do Estado, com base no registro de ocorrência policial desses indivíduos ou de outra fonte de informação oficial, tendo como objetivo a sua identificação a fim de oferecer a estes meios legais para libertá-los do vício. Essa legislação definiu, ainda, que o nome dessas pessoas poderia ser excluído da lista após requerimento, mas mediante laudo médico ou informação oficial atestando a não reincidência.

De acordo com o procurador-geral da República, autor da ação, a referida lei não foi específica em seus objetivos, buscando apenas tornar conhecidas, no meio policial, as pessoas que já foram detidas com substâncias entorpecentes, estigmatizando-as e excluindo-as no meio social, incorrendo, por consequência, essa legislação em grave ofensa ao direito à intimidade e à vida privada dos indivíduos incluídos em tal cadastro.

Além disso, de acordo com o autor, essa lei teria sido editada por ente federativo incompetente para tratar de matéria penal e processual penal, cuja competência legislativa é privativa da União, conforme previsão do art. 22, I, da Constituição Federal.

Em consonância com os argumentos do autor, o Ministro Edson Fachin, relator desse processo, reconheceu, em seu voto, a inconstitucionalidade formal dessa norma, por entender que, de fato, ela violava o disposto no art. 22, I, da Carta Constitucional, assemelhando-se esse cadastro "ao extinto rol de culpados de que tratava o art. 393, I, do Código de Processo Penal, como efeito da sentença condenatória, matéria, pois, tipicamente processual" (STF, 2020, on-line).

Ademais, segundo o Ministro, essa sistematização de dados seria competência da União, que já instituiu, através do art. 3º, I, da Lei federal nº 11.343/2006, o Sistema Nacional de Políticas Públicas sobre Drogas (Sisnad), que tem como finalidade a organização e coordenação de atividades relacionadas à prevenção do uso de drogas e reinserção social de usuários e dependentes[80], o que impede que os Estados criem um cadastro próprio.

Ainda de acordo com essa decisão, a Lei 3.528/2019, do Estado do Tocantins, teria também violado direitos fundamentais desses indivíduos, como a intimidade, a honra e a imagem, não preservando ainda a sua autonomia privada e autodeterminação, uma vez que essa

[80] Aduz esse dispositivo: "O Sisnad tem a finalidade de articular, integrar, organizar e coordenar as atividades relacionadas com: I - a prevenção do uso indevido, a atenção e a reinserção social de usuários e dependentes de drogas" (BRASIL, 2006).

norma não previu formas de controle e proteção desses dados nem o consentimento dos usuários e dependentes de drogas para a inclusão de seus nomes no cadastro.

Ao reconhecer a importância do tratamento de dados e sua atual contribuição para a reconfiguração do constitucionalismo brasileiro e para a atualização dos princípios constitucionais, o Ministro Edson Fachin afirmou, *in verbis:*

> [...] a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, traz em seu bojo o princípio da autodeterminação informativa (art. 2º, II) e a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV), a partir da concretização de princípios constitucionais que já se encontram plenamente em vigor na ordem jurídico brasileira. Ali, dados referentes à saúde são classificados como "dados pessoais sensíveis" (art. 5º, II) e, por isso, seu tratamento submete-se a um regime jurídico especial (art. 11). Esse sistema constitucional especial de proteção é violado pela lei impugnada, a qual, ademais, **não prevê formas de controle prévio à inclusão no cadastro, não prevê a comunicação e o consentimento do interessado** e, para a sua exclusão, exige laudo médico e informação oficial sobre a não reincidência. **Tampouco existe protocolo claro de proteção e tratamento desses dados**. (STF, 2020, on-line) (grifo nosso)

Mostrando, ainda, preocupação com a possibilidade de estigmatização e discriminação de usuários e dependentes de drogas com a criação desse cadastro, continuou esse Relator:

> Ao prever a alimentação do cadastro a partir de "registro de ocorrência policial ou de outra fonte de informação oficial", com nome do usuário ou dependente, nome da droga em sua posse, a forma de aquisição e outras informações de caráter reservado, pretende indevidamente individualizar e selecionar o usuário ou dependente de droga. Essa classificação ofende a isonomia ao segmentá-lo socialmente. Trata-se da primeira e clássica dimensão da igualdade que proíbe discriminações indevidas (STF, 2020, on-line).

Por tais razões, entendeu-se que a Lei 3.528/2019, do Estado do Tocantins, padecia não só de inconstitucionalidade formal, mas também material, tendo o STF, por maioria, concedido medida cautelar com vistas a suspender a sua eficácia, em decisão que ficou assim ementada:

> MEDIDA CAUTELAR. AÇÃO DIRETA DE INCONSTITUCIONALIDADE. LEI 3.528 DE 2019 DO ESTADO DO TOCANTIS. CADASTRO ESTADUAL DE USUÁRIOS E DEPENDENTES DE DROGAS. INCONSTITUCIONALIDADE FORMAL. MATÉRIA PENAL E PROCESSUAL PENAL. DIRETO SANITÁRIO. DIREITOS FUNDAMENTAIS. AFRONTA À NORMA FEDERAL. LEI 11.343/2006. COMPETÊNCIA DA UNIÃO PARA SISTEMATIZAÇÃO DE INFORMAÇÕES. INCONSTITUCIONALIDADE MATERIAL. DEFERIMENTO. 1. A norma é formalmente inconstitucional, uma vez que, ao criar o Cadastro Estadual de Usuários e Dependentes de Drogas (art. 1º) no âmbito da Secretaria Estadual de Segurança Pública com informações concernentes ao registro de ocorrência policial (§1º), inclusive sobre reincidência (§4º), invade competência privativa da União para legislar sobre matéria penal e processual penal (CRFB, art. 22, I). 2. Ademais, o exercício da competência concorrente em matéria de direito sanitário (CRFB, art. 24, XII), no federalismo cooperativo, deve maximizar direitos fundamentais e não pode ir de encontro à norma federal. No caso, nos termos da Lei federal n. 11.343/2006, a

> sistematização de informações é competência da União (art. 8º-A, XII). 3. Materialmente, também há inconstitucionalidade. **A seletividade social do cadastro é incompatível com o Estado de Direito e os direitos fundamentais que a Constituição de 1988 protege, especialmente, a igualdade (CRFB, art. 5º, caput), a dignidade da pessoa humana (CRFB, art. 1º, III), o direito à intimidade e à vida privada (CRFB, art. 5º, X) e o devido processo legal (CRFB, art. 5º, LIV). Inexistência tampouco de protocolo claro de proteção e tratamento desses dados**. 4. Medida cautelar em Ação Direta de Inconstitucionalidade concedida para suspender a lei impugnada. (STF - ADI 6561 MC, Relator(a): EDSON FACHIN, Tribunal Pleno, julgado em 13/10/2020, PROCESSO ELETRÔNICO DJe-260 DIVULG 28-10-2020 PUBLIC 29-10-2020) (STF, 2020, on-line) (grifo nosso)

Depreende-se, portanto, de tais julgados a importância da jurisprudência do Supremo Tribunal Federal para a temática da proteção de dados no Brasil e a contribuição desta Corte para o seu reconhecimento como um direito fundamental.

Espera-se, assim, que tais decisões tenham o condão de contribuir também para o amadurecimento dos debates acerca da sua fundamentalidade, enquanto esse direito não integra o catálogo de direitos e garantias fundamentais da nossa Constituição Federal. A sua afirmação como tal certamente garantirá maior segurança na coleta e utilização de dados pessoais e fortalecerá a posição da pessoa nesse contexto econômico e político repleto de desigualdades, assegurando a efetiva participação dos indivíduos na vida social.

CONCLUSÃO

Observou-se no presente estudo que, após a inserção das tecnologias de informação e comunicação no cotidiano dos indivíduos, cada vez mais, passamos a viver numa sociedade governada por dados. A circulação praticamente incessante de informações e as novas demandas mercadológicas que transformaram o modelo tradicional de negócio, antes focado basicamente na troca de bens ou serviços por uma quantia pecuniária, acabaram tornando os dados pessoais um novo ativo econômico.

Atualmente, é difícil imaginar uma empresa que não trabalhe direta ou indiretamente com dados pessoais e, a depender do negócio, estes se mostram vitais até para o seu próprio funcionamento. Com eles, é possível obter informações sobre hábito de consumo, perfis de consumidores e, assim, criar estratégias de *marketing* e publicidade que transformam os dados em instrumentos de geração de riquezas, dado o seu potencial mercadológico.

O próprio Poder Público, nas suas relações com o cidadão, também utiliza dados pessoais a fim de viabilizar a prestação dos seus serviços, programar políticas públicas e, a exemplo do que já acontece em alguns países, essas informações pessoais ainda são utilizadas para finalidades de proteção da sociedade contra crimes, para prevenção de doenças e com o objetivo de manter a constante vigilância sobre os indivíduos.

A multiplicação de bancos de dados contendo as mais variadas informações sobre as pessoas para fins diversos tem chamado a atenção, ao longo dos anos, para o desequilíbrio social resultante desse fenômeno, ocasionado pela assimetria existente na relação entre os titulares de dados e os entes privados e públicos que realizam a coleta e o tratamento destes. O potencial risco no uso indevido dessas informações, que pode causar a segmentação e a discriminação dos indivíduos, levando à violação de direitos fundamentais como a liberdade, a privacidade e a intimidade, tem ampliado sobremaneira os olhares à necessidade de proteção desses dados e, consequentemente, das pessoas, visando impedir a lesão a esses direitos e ao livre desenvolvimento da personalidade.

O ponto de partida para essa tutela surgiu, primeiramente, com o reconhecimento do direito à autodeterminação informativa no direito europeu, que influenciou fortemente o modelo de proteção de dados no Brasil. Esse direito, que consiste no poder dado ao indivíduo de controlar o uso dos seus dados e se baseia na ideia de consentimento do interessado, significou um importante marco nessa matéria, ainda na década de 80, quando, a partir daí,

foram desenvolvidas diversas legislações que buscaram conciliar os interesses econômicos com a proteção da pessoa e de seus valores fundamentais.

A ampliação da ideia de privacidade que, paulatinamente, culminou no reconhecimento da autonomia de um direito à proteção de dados, com normas e princípios próprios, desvencilhado daquele primeiro, levou também à inclusão, no sistema jurídico europeu, do direito à proteção de dados na categoria de direitos fundamentais, tendo em vista o seu poder social e a sua transformação num elemento essencial para o exercício da cidadania.

Com os crescentes debates sobre a importância e a regulamentação da matéria a nível nacional, essa discussão também ganhou relevo na doutrina brasileira, principalmente com a edição da Lei 13.709/2018, que, pela primeira vez, trouxe regras e princípios específicos sobre proteção de dados e trouxe o consentimento livre e inequívoco como vetor principal, a exemplo do modelo europeu, contribuindo para fortalecer a participação do indivíduo no processo de coleta e tratamento das suas informações. Não à toa, foi aprovada pelo Senado Federal, mas ainda pendente de julgamento pela Câmara dos Deputados, a Proposta de Emenda à Constituição nº 17 de 2019, que visa acrescentar o inciso XII-A ao artigo 5º, e o inciso XXX ao artigo 22, da Constituição Federal, incluindo a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

De qualquer forma, a despeito do reconhecimento da proteção de dados como um direito fundamental implícito já ser fortemente defendido por doutrinadores pátrios, buscou essa dissertação fazer uma análise mais aprofundada desse direito à luz da Constituição Federal e tomando como base os princípios e fundamentos trazidos pela Lei 13.709/2018, a fim de construir a sua estrutura dogmática enquanto um direito fundamental.

Por se tratar, portanto, de direito não expresso no texto constitucional, esse estudo tentou identificar a sua fundamentalidade material a partir de normas definidoras de direitos e garantias fundamentais e arriscou demonstrar que a legislação infraconstitucional, no caso a Lei 13.709/2018, também pode servir como fonte de um direito materialmente fundamental à proteção de dados, uma vez que foi essa legislação que inaugurou um sistema jurídico de tutela e de valores específicos no tocante à matéria, não sendo possível, portanto, desprender a sua análise do contexto desse trabalho.

Seguindo esse raciocínio, passou-se à investigação da dimensão subjetiva e objetiva desse direito fundamental implícito bem como ao estudo do seu âmbito de proteção e da sua titularidade, sem esquecer de observar o tratamento jurisprudencial do tema, numa tentativa de

fornecer elementos teóricos para a construção desse entendimento, contribuindo, assim, com a doutrina relacionada à matéria.

Dessa forma, foi possível verificar que o direito fundamental à proteção de dados, na sua dimensão subjetiva, pode ser configurado como um direito de defesa, na medida em que se caracteriza como um dever de abstenção imposto ao Estado para que este não interfira na esfera de liberdade e privacidade dos indivíduos, não podendo, assim, o ente estatal utilizar dados pessoais do cidadão para fins de controle, discriminação ou como instrumento de poder, reduzindo a proteção de outros direitos fundamentais.

E mesmo quando necessária a coleta dessas informações, deve o poder público e até mesmo o ente privado, se considerada a eficácia horizontal desse direito fundamental, observar estritamente os princípios norteadores do direito à proteção de dados, como a finalidade e a transparência, por exemplo, bem como os regramentos específicos dispostos na Lei 13.709/2018, sempre pautando suas ações pelo respeito à autodeterminação informativa. Ou seja, deve-se ter em mente que, a todos os indivíduos, cabe uma participação ativa e consciente em todo o processo de tratamento dos seus dados. Assim, nesse sentido, o direito fundamental à proteção de dados se mostra como uma limitação tanto da ação do Estado como dos entes privados.

Ele também se caracteriza como um direito a prestações fáticas, por impor ao Estado a obrigação de tomar medidas que assegurem a efetiva proteção dos indivíduos em relação aos seus dados, retirando seu fundamento dos direitos subjetivos extraídos tanto da Lei 13.709/2018 como do texto constitucional. Da mesma forma, é também um direito a prestações jurídicas, por obrigar o ente estatal à edição de normas, seja de organização seja de procedimento, que visem à concretização do exercício desses direitos, a exemplo da lei supracitada, que regulamenta de forma específica a atividade de coleta e de tratamento dos dados pessoais, definindo não só os limites dessa operação como também criando condições materiais para que os indivíduos possam exercer a sua autodeterminação informativa.

Já numa perspectiva objetiva, o direito à proteção de dados se desdobra ainda num dever de proteção, que exige do Estado a adoção de medidas positivas que reforcem a sua efetividade e a proteção dos demais direitos fundamentais a ele correlatos, sendo exemplo desse dever as normas de procedimentos administrativos previstas na Lei 13.709/2018 para a salvaguarda dos dados pessoais bem como a criação da Autoridade Nacional de Proteção de Dados (ANPD), órgão que tem a função de zelar pela proteção dos dados, fiscalizando as operações de tratamento e aplicando as sanções necessárias, em caso de uso indevido destes.

Nessa análise da dupla dimensão do direito fundamental à proteção de dados, foi possível extrair da Lei 13.709/2018 outros importantes mecanismos de defesa e de proteção que buscam garantir as condições necessárias para uma circulação de dados segura para o cidadão, que compreendidos e aplicados em conformidade com outros direitos fundamentais e valores dispostos na Constituição Federal, denotam a sua fundamentalidade material.

Reforça, ainda, essa fundamentalidade o fato de o direito à proteção de dados, a exemplo de outros direitos fundamentais, estar intrinsecamente conectado à dignidade da pessoa humana – não à toa, os titulares desse direito são todas as pessoas naturais –, e vincular diretamente os poderes legislativo, executivo e judiciário, impondo a estes um dever de respeito, proteção ou promoção desse direito, através de abstenções ou ações positivas que busquem a sua máxima eficácia e a constante tutela da pessoa.

Assim, nesse contexto, o indivíduo assume sempre um papel principal, cabendo, portanto, ao Estado e a qualquer ente privado coletor de dados a observância também dos direitos fundamentais que têm o indivíduo como seu núcleo principal de proteção, tais como a privacidade, a intimidade, a liberdade, a igualdade e o livre desenvolvimento da personalidade humana, com os quais o direito à proteção de dados possui intersecção e de onde ele extrai a sua essência. Por tais razões, a sua inserção como um direito fundamental autônomo se justificaria, uma vez que seu objeto imediato de tutela é a pessoa humana, que deve ser protegida das violações decorrentes do uso indevido de informações pessoais.

Constatou-se ainda, na presente dissertação, que a identificação de um direito materialmente fundamental à proteção de dados pode advir também de uma construção jurisprudencial, conforme se depreende da recente decisão prolatada pelo Supremo Tribunal Federal, nos autos da ADI nº 6387, que representou um marco na disciplina de proteção de dados no Brasil e uma clara limitação ao poder estatal, seguindo uma trilha já esperada por esse direito, a exemplo do que ocorreu na União Europeia, que deve culminar na aprovação da PEC 17/2019.

Percebe-se, assim, nesse estudo, que o direito à proteção de dados é fruto de uma natural evolução social e normativa decorrente de um desenvolvimento tecnológico que acabou transformando os dados em importante ativo econômico, fazendo gerar uma demanda crescente por uma tutela específica dos seus titulares, que estão sujeitos diariamente a inúmeros riscos de violação à sua privacidade.

Entretanto, a despeito de já existir uma legislação própria sobre a matéria, mostra-se necessária sua elevação à categoria de direitos fundamentais, como forma de estabelecer de

forma clara, no texto constitucional, o seu âmbito de proteção e os limites constitucionais à intervenção estatal, assegurando, dessa forma, as liberdades fundamentais do indivíduo e promovendo maior segurança jurídica no ordenamento jurídico brasileiro, na medida em que a positivação formal de um direito fundamental à proteção de dados carrega consigo uma carga positiva adicional de proteção.

REFERÊNCIAS

ALEMANHHA. Tribunal Constitucional Federal. **Resumo da sentença do Tribunal Constitucional Federal Alemão de 15 de dezembro de 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CÓDIGOS]**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html;jsessionid=CFBE0153659904890C268B9052A502A7.2_cid386. Acesso em: 07 set. 2020.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros Editores, 2006.

BENETT, Colin, J. The european general data protection regulation: an instrument for the globalization of privacy standards? **Information Polity,** n. 23, p. 239–246, 2018. DOI 10.3233/IP-180002

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho. Nova ed. Rio de Janeiro: Elsevier, 2004.

BONAVIDES, Paulo. **Curso de direito constitucional**. 19. ed., São Paulo: Editora Malheiros, 2006.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituição compilado.htm. Acesso em: 01 jul. 2020.

_____. Lei nº 8.078, de 11 de setembro de 1990. **Código de defesa do consumidor.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 nov. 2020.

_____. Lei nº 10.406, de 10 de janeiro de 2002. **Código civil**. Diário Oficial da União, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm. Acesso em: 01 jul. 2020.

_____. Lei nº 12.414, de 09 de junho de 2011. **Lei do cadastro positivo.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 10 nov. 2020.

_____. Lei nº 12.965, de 23 de abril de 2014. **Marco civil da internet.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 nov. 2020.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 jul. 2020.

_____. Medida Provisória nº 954, de 17 de abril de 2020b. **Diário Oficial da União.** Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 01 jul. 2020.

_____. Senado Federal. **Proposta de emenda à constituição n° 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. De autoria do Senador Eduardo Gomes (MDB/TO) (1º signatário) et al. Parte integrante do Avulso da PEC nº 17 de 2019. 2019a. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7925004&ts=1606766520897 &disposition=inline. Acesso em: 15 set. 2020.

_____. Superior Tribunal de Justiça. **Decisão STJ/MG.** Rrecurso especial. Fundamento não impugnado. Súm. 283/STF. Ação de compensação de dano moral. Banco de dados. Compartilhamento de informações pessoais. Dever de informação. Violação. Dano moral *in re ipsa*. Julgamento: CPC/15. (STJ. resp 1758799/MG, Rel. Ministra Nancy Andrighi, terceira turma, julgado em 12/11/2019, DJe 19/11/2019). 2019b Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019. Acesso em: 17 set. 2020.

_____. Supremo Tribunal Federal. **Ação direta de inconstitucionalidade 5.527 Distrito Federal**. Voto da ação de fiscalização abstrata a higidez constitucional dos artigos da Lei n. 12.965, de 23 de abril de 2014, o chamado Marco Civil da Internet, mais precisamente o seu artigo 10, em seu § 2º e o art. 12 em seus incisos III e IV. Relatora Ministra Rosa Weber. Brasília, 28 de maio de 2020. 2020c. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf. Acesso em: 01 jun. 2020.

_____. Supremo Tribunal Federal. **Arguição de descumprimento de preceito fundamental**. Relator Ministro Edson Fachin. Brasília, 28 de maio de 2020. 2020d. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. Acesso em 01 jun. 2020.

_____. Supremo Tribunal Federal. **Medida cautelar na ação direta de inconstitucionalidade 6.387**. Medida cautelar em ação direta de inconstitucionalidade proposta pelo Conselho Federal da Ordem dos Advogados do Brasil – CFOAB contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020a". Relatora Ministra Rosa Weber. Brasília, 24 de abril de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em 01 jun. 2020.

CASTELLS, Manuel. **A sociedade em rede**. 20. ed. revisada e ampliada. São Paulo: Paz e Terra, 2019.

CHILE. Ministerio Secretaría General de la Presidencia. **Ley 21096**. Consagra el derecho a protección de los datos personales. Biblioteca Nacional do Chile. Publicada em 16 jun. 2018. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1119730. Acesso em: 16 set. 2020.

CONSELHO DA EUROPA (DdE). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. **European Treaty Series**. n. 108, Strasbourg, 28.I. 1981. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em 10 set. 2020.

COSTA, R. S.; OLIVEIRA, S. R. **Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais.** Revista Brasileira de Direito Civil em Perspectiva | e-ISSN: 2526-0243 | Belém | v. 5 | n. 2 | p. 22 - 41 | Jul/Dez. 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico de Direito. Joaçaba, v.12, n.2, p.91-108, jul.-dez. 2011. Disponível em: https://dialnet.unirioja.es/revista/12418/A/2011. Acesso em: 01 jul. 2020.

_____. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

_____. **Privacidade e transparência no acesso a informação pública**. In: Democracia eletrônica. MEZZAROBA, Oribes; GALINDO, Fernando. Espanha (Zaragoza): Prenzas Universitarias de Zaragoza, 2010.

ESPANHA. Palácio da Moncloa. **Constituição Espanhola**. Aprovada pelas Cortes Gerais em 31 de outubro de 1978. Ratificada por Referendum Popular em 6 de dezembro de 1978. Sancionada por sua Majestade o Rei Don Juan Carlos I frente às Cortes Gerais em 27 de dezembro de 1978. (B.O.E., n.º 311-1, de 29 de diciembre de 1978). Reforma do artigo 13, item 2, da Constituição Espanhola, de 27 de agosto de 1992. (B.O.E., n.º 207, de 28 de agosto de 1992), 1992. Disponível em: https://www.tribunalconstitucional.es/es/tribunal/normativa/Normativa/CEportugu%C3%A9s.pdf. Acesso em: 15 set. 2020.

_____. Tribunal Constitucional Espanhol. **Acórdão 76/2019, de 22 de maio de 2019**. BOE (Official State Gazzete), n. 151, de 25 de junho de 2019. Disponível em: https://hj.tribunalconstitucional.es/en/Resolucion/Show/25942. Acesso em: 20 set. 2020.

FERRAJOLI, Luigi. **Derechos y garantias: la ley del más débil**. Tradução para o espanhol: Perfecto Andrés Ibánez e Andrea Greppi. Madri: Editorial Trotta, 1999.

FRAZÃO, Ana. Objetivos e alcance da lei geral de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil. 2019.

GUIDI, Guilherme Berti de Campos. **O papel do consentimento para a proteção de dados pessoais**: União Europeia, Estados Unidos e Brasil. Direito internacional em expansão. v. XVI. Belo Horizonte: Arraes Editores, 2019. ISBN: 978-858238-642-2.

HÄBERLE, Peter. **Hermenêutica constitucional:** a sociedade aberta dos intérpretes da Constituição: contribuição para a interpretação pluralista e procedimental da constituição. Tradução de Gilmar Ferreira Mendes. Porto Alegre: Sérgio Antônio Fabris Editor, 1997.

HESSE, Konrad. **Temas fundamentais do direito constitucional**. São Paulo: Saraiva, 2009.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The population census decision and the right to informational self-determination. **Computer Law & Security Report.** v. 25, n. 1, 2009. Disponível em: https://www.uni-kassel.de/fb07/fileadmin /datas/fb07/5-Institute/IWR/Hornung/Hornung___Schnabel__Data_protection_in_Germany _I__CLSR_2009__84.pdf. Acesso em: 08 set. 2020.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **PNAD contínua**. 2020. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/trabalho/17270-pnad-continua.html?=&t=o-que-e. Acesso em: 01 jun. 2020.

KELSEN, Hans. **Teoria pura do direito**. Tradução de João Baptista Machado. 6. ed. São Paulo: Martins Fontes, 1998.

LESSA, Célia. **O Estado do bem-estar social na era da razão**. Rio de Janeiro: Elsevier, 2012.

MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Prefácio de Jan Woischnik. Tradução de Beatriz Hennig et al. Montevidéu: Fundação Konrad Adenauer, 2005.

MENDES, Gilmar Ferreira. **Curso de direito constitucional**. 14. ed. rev. e atual. São Paulo: Saraiva Educação, 2019.

_____. **Direitos fundamentais: eficácia das garantias constitucionais nas relações privadas**. In: GRUNDMANN, Stefan et al. Direito privado, constituição e fronteiras, 2. ed. São Paulo: Revista dos Tribunais, 2014a.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gonet. **Curso de direito constitucional**. São Paulo: Saraiva Educação, 2019.

MENDES, Laura Schertel. **Habeas data e autodeterminação informativa: os dois lados da mesma moeda**. Revista Direitos Fundamentais & Justiça. Belo Horizonte, ano 12, n. 39. 2018.

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

MULHOLLAND. Caitlin. **Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18).** Revista de direitos e garantias fundamentais. Vitória, v. 19, n. 3. 2018, p. 159-180. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 05 dez. 2020.

MULHOLLAND. Caitlin. **O direito de não saber como decorrência do direito à intimidade**. civilistica.com. a. 1, n. 1, 2012. Disponível em: http://civilistica.com/wp-content/uploads/2015/02/Mulholland-civilistica.com-a.1.n.1.2012.pdf. Acesso em: 05 jun. 2020.

NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa**. Laboratório de Estudos Teóricos e Analíticos sobre o Comportamento das Instituições (LETACI), vinculado à Faculdade Nacional e ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio de Janeiro, com financiamento da Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) pela concorrência do Edital nº 9 de 2011 (Processo nº E26/111.832/2011), e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pela concorrência do Edital Universal de 14/2011 (Processo n° 480729/2011-5) Disponível em: http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c. Acesso em 11 nov. 2020.

OLIVEIRA, Ana Paula de; ZANETTI, Dânton. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR**. ano 4, n. 1. mai. 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 01 jun. 2020.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf >. Acesso em: 9 jun. 2020.

PARLAMENTO EUROPEU. **Carta dos Direitos Fundamentais da União Europeia**. Jornal Oficial das Comunidades Europeias. 18.02.200. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 20 set. 2020.

_____. **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. Jornal Oficial nº L 281 de 23/11/1995 p. 0031 – 0050, 1995.

_____. **Directiva 2002/58/CE do Parlamento Europeu e do Conselho**, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Jornal Oficial nº L 201 de 31/07/2002, p. 0037 – 0047, 2002.

_____. **Regulamento (Ue) 2016/679 do Parlamento Europeu e do Conselho.** de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 15 set. 2020.

PIEROTH, Bodo; SCHLINK, Bernhard. **Direitos fundamentais**. Tradução de António Francisco de Sousa e António Franco. São Paulo: Saraiva, 2011.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

PORTUGAL. Assembleia da República. **Constituição da República Portuguesa**. Promulgada em 2 de abril de 1976. Sétima Revisão Constitucional [2005]. Disponível em: https://www.parlamento.pt/Legislacao/Documents/constpt2005.pdf. Acesso em: 02 jul. 2020.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A proteção de dados pessoais na internet no brasil: análise de decisões proferidas pelo Supremo Tribunal Federal**. Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. v. 11, n. 2, 2016. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936. Acesso em 01 jun. 2020.

RAMIRO, Mônica Arenas. **El derecho fundamental a la protección de datos p ersonales em Europa.** Valencia: Tirant la blanch, 2006.

REINHARDT. Jörn. **Conflitos de direitos fundamentais entre atores privados**: "efeitos horizontais indiretos" e pressupostos de proteção de direitos fundamentais. Belo Horizonte, ano 13, n. 41, p. 59-91, jul.-dez. 2019. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/819. Acesso em 01 jun. 2020.

RIO GRANDE DO SUL. Tribunal de Justiça do Rio Grande do Sul. **Decisão apelação cível: apelação cível nº 70069420503**. Sexta Câmara Cível. Relator: Desembargador Ney Wiedemann Neto. Julgado em: 25-08-2016). Disponível em : https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html. php. Acesso em: 10 set. 2020.

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

RUARO Regina Linden; RODRIGUEZ Daniel Piñeiro; FINGER Brunize**. O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito-UFPR, Curitiba, n. 53, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768/19876. Acesso em: 01 jul. 2020.

SARLET, Ingo Wolfgang. **A Eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. e atual. Porto Alegre: Livraria do Advogado Editora, 2018.

_____. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Revista Direitos Fundamentais & Justiça. Belo Horizonte, ano 14, n. 42, 2020.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 25. ed. rev. e atual. São Paulo: Malheiros Editores, 2005.

TEPEDINO, G.; FRAZÃO, A.; OLIVA, M. D. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

VERGILI. Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei**

Geral de Proteção de Dados. Dataprivacy. Artigos 18.09.2019, 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados/. Acesso em: 05 jun. 2020.