UNIVERSIDADE DE BRASÍLIA (UnB)

Faculdade de Direito (FD)

Curso de Graduação em Direito

BRUNO FERNANDES DE PAULA

VIGILÂNCIA ESTATAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

Uma análise do Decreto nº 10.046/2019 à luz do paradigma constitucional da proteção de dados pessoais

STATE SURVEILLANCE AND THE FUNDAMENTAL RIGHT TO PROTECTION OF PERSONAL DATA:
An analysis of Decree No. 10.046/2019 from the constitutional paradigm of personal data protection

Brasília
2021

UNIVERSIDADE DE BRASÍLIA (UnB)

Faculdade de Direito (FD)

Curso de Graduação em Direito

VIGILÂNCIA ESTATAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS:

Uma análise do Decreto nº 10.046/2019 à luz do paradigma constitucional da proteção de dados pessoais

Autor: Bruno Fernandes de Paula

Orientadora: Prof. Dra. Laura Schertel Mendes

Monografia apresentada à Banca Examinadora, na Faculdade de Direito da Universidade de Brasília, como requisito parcial à obtenção do título de Bacharel em Direito.

Brasília, 1º de outubro de 2021.

FOLHA DE APROVAÇÃO

BRUNO FERNANDES DE PAULA

Vigilância estatal e o direito fundamental à proteção de dados pessoais: uma análise do Decreto nº 10.046/2019 à luz do paradigma constitucional da proteção de dados pessoais

Monografia apresentada como requisito parcial à obtenção do grau de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD/UnB).

Aprovada em: ___ de _____ de 2021.

BANCA EXAMINADORA

_____

Prof. Dra. Laura Schertel Ferreira Mendes

(**Orientador – Presidente**)

_____

Prof. Dr. Danilo Cesar Maganhoto Doneda

(**Membro Avaliador**)

_____

Gabriel Campos Soares da Fonseca

(**Membro Avaliador**)

Ao meu eterno primo **Robson Marcos de Paula.**

AGRADECIMENTOS

Sem dúvidas, o ato individual de escrita deste trabalho é contrastante com a coletividade de pessoas que estiveram por trás – de forma essencial – em todo caminho até aqui. Dessa forma, não há como não mencionar, em primeiro lugar, Wilson e Ana Paula, pais dedicados muito além do que para o provimento de toda estrutura material proporcionada, mas, principalmente, empenhados – com êxitos – em prover o que há de mais humano em mim, minha índole e moral. Ao lado deles, meus irmãos, Hugo e Caio, formam a fortaleza e a base mais valiosa que tenho na vida.

Ainda no seio familiar, agradeço aos meus amados "voinhos". Vó Florinda e vô Paulo sempre ocuparam posição de referência para mim. É certo que sem a constante presença dos dois na minha vida – cheia de amor e carinho – eu não seria quem sou hoje.

Ana Letícia é mais do que merecedora dos meus agradecimentos, é responsável também por tudo que conquistei até aqui. Há quase oito anos juntos, foi minha principal companheira e incentivadora, caminhando, lado a lado, desde a fase de estudo e empenho para o vestibular e estando junto para tudo que a vida nos apresentou, sejam situações positivas ou negativas. É fonte inesgotável de inspiração, cumplicidade, amizade e amor.

Também merecem agradecimentos especiais meus grandes amigos da Faculdade de Direito, Luís Carlos e Gabriel Fonseca. Luís, desde a época de escola, esteve ao meu lado, acreditou em mim e vibrou a cada conquista. Gabriel, também depositando grande confiança, proporcionou minha principal experiência profissional e grandes aprendizados, bem como é o principal responsável pela a aproximação com a área jurídica que, hoje, tenho grande apreço e sobre a qual desenvolvo este trabalho: a proteção de dados. Os dois são pessoas pelas quais tenho grande honra e orgulho em chamar de amigos e que sempre irei me espelhar profissionalmente.

Por fim, ao grande grupo de amigos que, felizmente, me cerca, agradeço com toda sinceridade. Todos foram essenciais até aqui, por todas conversas, reflexões e diversões. Sem minhas amizades, eu não teria capacidade de todo o esforço desempenhado: são "válvulas de escape" que renovam constantemente minha energia e vontade.

FICHA CATALOGRÁFICA:

de Paula, Bruno Fernandes
dD278
VIGILÂNCIA ESTATAL E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS: Uma análise do Decreto nº 10.046/2019 à luz do paradigma constitucional da proteção de dados pessoais / Bruno Fernandes de Paula; orientador Laura Schertel Ferreira Mendes. -- Brasília, 2021.

80 p.

1. . I. Mendes, Laura Schertel Ferreira, orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA:

DE PAULA, Bruno Fernandes. **Vigilância estatal e o direito fundamental à proteção de dados pessoais:** uma análise do Decreto nº 10.046/2019 à luz do paradigma constitucional da proteção de dados. Monografia de Final de Curso em Direito, Faculdade de Direito, Universidade de Brasília, Brasília, DF, 2021, 80f.

RESUMO

O presente trabalho investiga, em termos gerais, o tratamento de dados pessoais no Poder Público, sob a lente do direito fundamental à proteção de dados, cuja autonomia foi reconhecida no julgamento na emblemática decisão *Volkszählungsurteil* da Suprema Corte alemã e na ADI nº 6.387/DF, no contexto nacional. Mais especificamente, a análise desempenhada neste trabalho busca responder se o Decreto nº 10.046/2019 (que dispõe "sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados") é compatível com as principais lições oriundas da referida garantia constitucional. Nesse intuito, os passos iniciais do trabalho consistem no estudo dogmático do direito fundamental à proteção de dados: em primeiro, a partir do exame de seus principais contornos delineados no direito alemão, um de seus principais berços; em segundo, mediante a apresentação do tratamento doutrinário e jurisprudencial brasileiro, que – embora atrasado – caminha com significativo progresso em relação ao tema. Dessa forma, com o marco teórico estabelecido, impende detalhada análise do Decreto nº 10.046/2019 para, assim, realizar o exame de constitucionalidade de seus principais dispositivos. Em conclusão, sustenta-se que o ato normativo editado pelo Governo Federal é deficiente em uma quantidade significativa de pontos e, portanto, configura-se como medida inconstitucional.

Palavras-chave: Direito Constitucional; Direito Fundamental; Proteção de Dados; Poder Público; Decreto nº10.046/2019.

ABSTRACT

This undergradaduate thesis investigates, in general terms, the processing of personal data in the Public Power, under the scrutiny of the fundamental right to data protection, whose autonomy was recognized in the judgment in the emblematic decision Volkszählungsurteil of the German Supreme Court and in ADI nº 6.387/DF, in the Brazilian context. More specifically, the analysis performed in this work seeks to answer whether Decree No. 10.046/2019 (which provides "on the governance of data sharing within the federal public administration and institutes the Citizen's Base Registry and the Central Data Governance Committee") is compatible with the main lessons arising from the aforementioned constitutional guarantee. To this end, the initial steps of the work consist of the dogmatic study of the fundamental right to data protection: first, from the examination of its main contours outlined in German law, one of its main cradles; secondly, through the presentation of the Brazilian doctrinal and jurisprudential treatment, which – although delayed – is progressing with significant progress in relation to the subject. Thus, with the established theoretical framework, a detailed analysis of Decree No. 10,046/2019 is required, in order to carry out the examination of the constitutionality of its main provisions. In conclusion, it is argued that the normative act issued by the Federal Government is deficient in a significant amount of points and, therefore, it is configured as an unconstitutional measure.

Keywords: Constitutional right; Fundamental right; Data Protection; Public Power; Decree No. 10,046/2019.

SUMÁRIO

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ABIN	Agência Brasileira de Inteligência
ADPF	Arguição de Descumprimento de Preceito Fundamental
ANPD	Autoridade Nacional de Proteção de Dados
BGHZ	*Bundesgerichtshof*
BVerfG	*Bundesverfassungsgerichts*
BVerfGE	*Entscheidungen des bundesverfassungsgerichts*
CBC	Cadastro Base do Cidadão
CCGD	Comitê Central de Governança de Dados
CF/1988 ou CF/88 ou CF	Constituição Federal de 1988
CFOAB	Conselho Federal da Ordem dos Advogados do Brasil
DENATRAN	Departamento Nacional de Trânsito
EUA	Estados Unidos da América
IBGE	Instituto Brasileiro de Geografia e Estatística
LGPD	Lei Geral de Proteção de Dados
MP	Medida Provisória
MS	Mandado de Segurança
OAB	Ordem dos Advogados do Brasil
PEC	Proposta de Emenda Constitucional
RE	Recurso Extraordinário
SERPRO	Serviço Federal de Processamento de Dados
STF	Supremo Tribunal Federal
TICs	Tecnologias de informação e comunicação
TRF	Tribunal Regional Federal
v.g.	*Verbi gratia*

INTRODUÇÃO

As origens e bases da disciplina da matéria de proteção de dados estão certamente ligadas ao direito à privacidade e seu desenvolvimento. Nesse contexto, os Estados Unidos da América tiveram papel central na formulação dessa garantia, mormente através do emblemático artigo "*The right to privacy"*, de Samuel Warren e Louis Brandeis, publicado em 1890, e compreendido na doutrina como o marco inicial do direito à privacidade[1].

A publicação científica teve êxito em enunciar o que chamou de *"right to be let alone"*, isto é, um espaço da vida íntima que deve ser inviolável. Todavia, o principal ponto para uma reflexão posterior da proteção de dados consistiu na associação do desenvolvimento tecnológico e a necessidade de tutela da privacidade. Nesse viés, destacou-se que "recentes invenções e novos métodos empresariais chamavam atenção para o próximo passo que precisa ser dado para a proteção da pessoa"[2]. É desse ponto de vista que o direito começa a considerar as invasões à vida íntima como importunos que devem ser limitados.

Diante do contexto em que o artigo se inseria, no final do século XIX, as violações as quais os autores fizeram referência consistiam principalmente em fotografias e notícias da vida íntima das pessoas, entendendo haver a necessidade de um âmbito de proteção bem individualista e específico a essas situações. Contudo, com o vertiginoso desenvolvimento tecnológico testemunhado durante o século XX, esse escopo da privacidade mostrou-se exíguo frente aos novos riscos.

Exemplos disso são os casos do *National Data Center* e *SAFARI*, respectivamente, nos EUA e na França, ocorridos nos finais da década de 1960 e início da década de 1970. Ambos tratam de propostas de órgãos técnicos dos Estados para a implementação de bancos de dados pessoais centralizados, a fim de promover maior eficiência da administração pública. Todavia, ante intensos debates públicos na época, as proposituras foram afastadas em razão dos riscos do acúmulo e tratamento de dados em um novo contexto tecnológico[3]. Visualizou-se, portanto,

---

[1] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 6.

[2] WARREN, Samuel; BRANDEIS, Louis. **The right to privacy.** Harvard Law Review, v. IV, n. 5, 1890, p. 195, tradução livre. ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person").

[3] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Renovar, 2006.

uma reinvenção do direito à privacidade, compreendido por uma lente de tutela mais coletiva e que fez emergir a proteção de dados pessoais[4].

Assim, um direito autônomo à proteção de dados começou a ser concebido. Merece destaque a edição do primeiro diploma normativo de proteção de dados pessoais do mundo, no Estado alemão de Hesse, em 1970. Demais disso, outro ponto emblemático e de grande relevância no desenvolvimento da matéria é a decisão do Tribunal Constitucional Federal alemão sobre o censo demográfico (*volkszählungsurteil*), em 1983. O precedente foi responsável pela consolidação do direito à autodeterminação informativa[5] (*informationelle Selbstbestimmung*) e será objeto de análise no desenvolvimento deste trabalho.

Por ora, vale destacar dois pontos do julgado. Primeiro, constata-se o êxito que teve em conceder guarida constitucional à proteção de dados pessoais. Sob o entendimento de que esses dados configuram uma projeção da personalidade do indivíduo, criou-se uma sólida base para a teoria da proteção de dados "ao reconhecer um direito subjetivo fundamental e alçar o indivíduo a protagonista no processo de tratamento de seus dados."[6]. Nesse sentido, a proteção de dados foi compreendida como garantia fundamental essencial para consecução de outros direitos constitucionais, como a dignidade da pessoa humana e o livre desenvolvimento da personalidade[7].

Em segundo lugar, o entendimento de que não há dados insignificantes é outro fruto da decisão de grande valia para a matéria de proteção de dados. Esse entendimento é fundado na constatação de que qualquer informação pessoal aparentemente inofensiva pode adquirir novos valores a partir do processamento automatizado.

---

[4] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014, p. 29.
Ainda, sobre a dimensão coletiva desenvolvida, vale destacar o seguinte trecho do Professor Ingo Wolfgang Sarlet: "e aqui a dimensão metaindividual (coletiva) – se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (right to be alone)." SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, jan./jun. 2020, p. 190. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.

[5] Segundo o próprio texto do julgado, o conteúdo deste direito traduz-se no poder de cada indivíduo "de decidir em princípio por si próprio, quando e dentro de que limites fatos pessoais serão revelados". SCHWABE, Jürgen; MARTINS, Leonardo. Decisão do Tribunal Constitucional alemão de 1983. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Konrad Adenauer Stiftung, 2005, pp. 237. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 11/03/2021.

[6] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014, p. 31.

[7] SCHWABE, Jürgen; MARTINS, Leonardo. Decisão do Tribunal Constitucional alemão de 1983. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Konrad Adenauer Stiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 11/03/2021.

Dessa forma, foi possível visualizar uma diferenciação entre a tutela da privacidade e da proteção de dados, propriamente dita. É que, apesar da associação e dedução entre os institutos, a proteção de dados consolidou-se com base em um conceito ampliado de dados, que vão além da esfera da vida íntima e privada do indivíduo[8]. Exemplo disso é o que Indra Spiecker gen. Döhmann, professora da Universidade de Frankfurt, chama de proteção de dados na esfera pública. É dizer: informações pessoais em praças públicas, escolas e locais de trabalho, por exemplo, também devem ser protegidas[9].

Nesse sentido, a doutrina entende que houve uma superação, uma vitória na direção da autonomia da proteção de dados em relação à privacidade, em que pese o contínuo laço e mutua referência entre essas garantias jurídicas. Aliás, identifica-se esse vínculo no compartilhamento dos mesmos fundamentos jurídicos em ambos institutos, quais sejam, a dignidade humana e proteção da personalidade[10].

Noutro giro, é de grande importância materializar nesta seção introdutória os graves riscos causados por possíveis violações no tratamento de dados pessoais. Nesse viés, em artigo científico[11], a professora Laura Schertel Mendes explora essa questão e seus impactos em outras garantias constitucionais. No que diz respeito às relações privadas, destacam-se como exemplos: (i) o uso das "listas negras", utilizadas para avaliar candidatos a vagas de emprego mediante constatação da sua presença ou não em cadastros de pessoas que ajuizaram ações trabalhistas, o que viola a liberdade de exercício de trabalho; (ii) a exigência de testes genéticos como requisito para contratação, condição que também viola a liberdade de exercício de trabalho; (iii) a proibição de viajar em aeronaves por ter o nome equivocadamente em listas de terroristas, o que resulta em violação ao direito de ir e vir e; (iv) ser importunado e ter a

---

[8] SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, pp. 179-218, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.
Nesse mesmo sentido, o especialista Bruno Bioni leciona (grifo nosso): "A dinâmica de proteção dos dados pessoais foge à dicotomia do público e do privado, diferenciando-se substancialmente do direito à privacidade. Propugnar que o direito à proteção dos dados pessoais seria uma mera evolução do direito à privacidade é uma **construção dogmática falha** que dificulta a sua compreensão." BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019. p. 95.

[9] DÖHMANN, Indra Spiecker genannt. A proteção de dados pessoais sob o regulamento geral. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 97-113.

[10] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014, p. 35.
[11] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 192-193, jul./dez. 2018.

liberdade de escolha reduzida por publicidade comportamental, geradas a partir da construção de perfis *(profiling)* por tratamento de dados pessoais sem o consentimento adequado, o que importa na violação do livre desenvolvimento da personalidade.

Por outro lado, em face da grande capacidade estatal e do seu monopólio do uso da força, entende-se neste trabalho que as violações no tratamento de dados perpetradas no âmbito do poder público são ainda mais gravosas e preocupantes. Adianta-se, aliás, que é esse o recorte selecionado sobre qual a presente monografia debruçar-se-á. A título de exemplo dos possíveis riscos causados por intervenções estatais irregulares nos dados pessoais, coloca-se: (i) a prática do *racial profiling* na segurança pública e no próprio judiciário, consistente na tomada de decisão discriminatória baseada em banco de dados que carregam informações pessoais sensíveis (*v.g.*, raça e imigração), resultando na violação do direito à igualdade e; (ii) o registro público acerca das participações públicas *(v.g.*, manifestações e protestos), que tem como provável efeito o desencorajamento de tal participação, minando a liberdade de reunião[12].

Em vista do último exemplo, já se evidencia que a proteção de dados é relevante não só para a garantia de direitos individuais, mas também para a próprio regime democrático. Outro abuso muito preocupante, nesse sentido, consiste na utilização de banco de dados pessoais poderosos para o desenvolvimento de *profilings* voltados a guiar a publicidade de candidatos e campanhas políticas, o que coloca em xeque o processo eleitoral.

Nesse contexto, o caso da *Cambridge Analytica*[13] é emblemático. Em 2018, ganhou grande repercussão na mídia que a referida empresa norte-americana utilizou de uma série de dados pessoais oriundos do *Facebook* para interferir decisivamente nas eleições americanas e no plebiscito sobre a saída do Reino Unido do Bloco da União Europeia (*Brexit*), ambas em 2016. O *modus operandi* consistiu no tratamento de dados pessoais coletados em pesquisas de personalidade na rede social para, assim, montar perfis e direcionar conteúdo específico para que um grupo mais suscetível se voltasse para a opção pretendida pelo contratante da empresa (estratégia conhecida como *microtargeting*).

Ainda, outra problemática flagrante, no contexto brasileiro, consiste na utilização de catálogos de fotos de suspeitos em delegacias para produção de provas criminais. Ocorre que

---

[12] *Ibidem.*

[13] CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. **New York Times.** New York, 4 abr. 2018 Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 13 mar. 2021

GUIMÓN, Pablo. "O 'Brexit' não teria acontecido sem a Cambridge Analytica". **EL PAÍS.** Londres, 16 mar. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html. Acesso em: 13 mar. 2021.

essa identificação fotográfica muitas vezes está sendo utilizada como único meio a evidenciar condutas ilícitas, justificando a prisão de inocentes[14]. Como agravante, constata-se que a coleta de fotos (dados pessoais) é muitas vezes procedida de modo descriterioso – por exemplo, retiradas de rede social – e, ainda, verifica-se claramente um viés discriminatório[15]. Todavia, o tratamento irregular de dados pessoais pela segurança pública não se restringe ao Brasil. Nos Estados Unidos, por exemplo, já se verificou caso de prisão equivocada em razão de prova produzida por algorítmico de reconhecimento facial[16].

Ante todos esses graves riscos, é patente a necessidade de uma rígida regulação sobre o tema. Por um lado, o aspecto constitucional da tutela dos dados pessoais é ponto que merece grande reflexão. Destaca-se que a Constituição Federal de 1988 não traz um direito autônomo e expresso nesse sentido, embora tal salvaguarda possa ser compreendida em outras garantias fundamentais, como a privacidade (art. 5º, X), a inviolabilidade das comunicações (art. 5º, XII) e o *habeas data* (art. 5º, LXXII). A importância da consolidação de um direito constitucional autônomo à proteção de dados pessoais consiste em, por exemplo, garantir um mecanismo de defesa contra novas legislações que, porventura, oponham-se à princípios gerais da matéria.

No campo infraconstitucional, mesmo que com atraso, o meio acadêmico e o poder público vêm se aprofundando na matéria. Nessa direção, destaca-se a edição da moderna Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), diploma normativo que tem forte inspiração no modelo europeu e colocou o Brasil no mapa dos países que regulam os dados pessoais de maneira uniforme e sistematizada.

Todavia, cumpre ressaltar que já havia estabelecida uma diversidade normativa que aborda relevantemente situações específicas de tratamento de dados. Para fins deste trabalho, vale destacar os diplomas normativos associados à atividade estatal, são eles: Lei de Interceptação Telefônica (Lei nº 9.296/1996), Lei de Organização Criminosa (Lei nº 12.850/2013) e Marco Civil da Internet (Lei nº 12.965/2014). Sobre esses diplomas normativos

---

[14] PAULUZE, Thaiza. Foto em delegacia faz jovem negro ser acusado 9 vezes e preso duas vezes por roubos que não cometeu. **Folha de São Paulo.** São Paulo 2 jan. 2021 Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/01/foto-em-delegacia-faz-jovem-negro-ser-acusado-9-vezes-e-preso-duas-por-roubos-que-nao-cometeu.shtml. Acesso em: 13 mar. 2021.
JUSTINO, Luiz Carlos da Costa. "QUAL FACÇÃO, VAGABUNDO?": O violoncelista inocente que ficou cinco dias preso. **Revista Piauí**, Edição 169, out. 2020. Disponível em: https://piaui.folha.uol.com.br/materia/qual-faccao-vagabundo/. Acesso em: 13 mar. 2021.

[15] Levantamento desenvolvido pelo Condege, organização de defensores público de todo o país, indicou que os negros representam 83% dos erros de identificação fotográfica no Brasil. Disponível em: https://g1.globo.com/fantastico/noticia/2021/02/21/exclusivo-83percent-dos-presos-injustamente-por-reconhecimento-fotografico-no-brasil-sao-negros.ghtml. Acesso em 13 mar. 2021.

[16] HILL, Kashmir. Wrongfully Accused by an Algorithm. **New York Times**. New York, 24 jun. 2020. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Acesso em 13 mar. 2021.

e suas respectivas adequações constitucionais, a doutrina e a jurisprudência já se debruçaram com afinco.

Noutra perspectiva, mais recentemente, o Governo Federal editou o Decreto nº 10.046/2019, que dispõe "sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.". Tal corpo normativo merece grande atenção em razão de sua amplitude e modernidade, além de que despertou críticas na opinião pública por supostas incongruências com preceitos gerais da proteção de dados. São essas circunstâncias que instigaram o desenvolvimento do presente trabalho, voltado para uma análise do Decreto nº 10.046 à luz dos fundamentos constitucionais da proteção de dados pessoais.

Diante desse cenário, o presente trabalho busca responder a seguinte pergunta: O Decreto nº 10.046/2019 editado pelo Governo Federal em 2019 é consonante com o moderno paradigma constitucional da proteção de dados? Já a hipótese central é a de que o instituto normativo apresenta disposições conflituosas com o que há de mais novel no tratamento constitucional da matéria, seja em âmbito doutrinário ou jurisprudencial, nacional ou internacional.

Demais disso, defende-se na monografia que, como leciona o cientista da computação Simson Garfinkel[17], há a viabilidade de ampliar a tecnologia e suas possibilidades sem com que haja uma correspondente redução na privacidade e proteção dos dados das pessoas. Tudo isso, registre-se, tendo em vista que essas garantias não são absolutas, isto é, há limitações de suas aplicações em face de outros direitos fundamentais.

Por fim, impende demonstrar que o trabalho será divido em três capítulos, com uma breve síntese sobre seus objetivos e estrutura no começo de cada um. O primeiro objetivará apresentar a construção da ideia constitucional da proteção de dados no direito alemão, principalmente por meio da exposição dos fundamentos de importantes precedentes da Corte Federal Constitucional da Alemanha. O segundo capítulo buscará um aprofundamento no tratamento constitucional brasileiro sobre a proteção de dados, evidenciando a posição doutrinária acerca da existência de um direito fundamental autônomo, bem como as principais

[17] O Professor faz uma interessante analogia do possível *trade-off* entre desenvolvimento tecnológico e privacidade com o desenvolvimento econômico e a questão ambiental. Nesses termos, o cientista afirma que, nas décadas de 1950 e 1960, acreditava-se que não havia possibilidades de desenvolver a economia sem impactar negativamente a natureza, tese que foi desconstruída com o surgimento de uma visão de desenvolvimento econômico sustentável. Assim, para o autor, da mesma forma acontece com a privacidade e a tecnologia, não havendo real impedimento do progresso dessa sem o retrocesso daquela. GARFINKEL, Simson. **Database Nation: the death of privacy in the 21th Century.** California: O'Reilly Media, 2000. p. 15.

decisões sobre o tema no Supremo Tribunal Federal (STF). Finalmente, posto o marco teórico do trabalho, o último capítulo incumbir-se-á de analisar o Decreto nº 10.046/2019 em face dos contornos dogmáticos do direito fundamental à proteção de dados construídos nos capítulos anteriores.

NOTAS METODOLÓGICAS

Primeiramente, em nome da integridade acadêmica, não poderia deixar de citar as limitações de pesquisa sobre o tema. Esse fato decorre, principalmente, da exiguidade do desenvolvimento doutrinário-dogmático do direito fundamental à proteção de dados pessoais no Brasil. É que, nada obstante as relevantes obras oriundas da doutrina brasileira, a contemporaneidade do reconhecimento da garantia implica em uma carência de pesquisa[18].

Além disso, há de se destacar que o "julgamento constitucional" do ato normativo, tal como escolhido, é apenas uma das formas possíveis de leitura ao Decreto nº 10.046/2019. Poder-se-ia, por exemplo, analisar o diploma normativo através da Lei nº 13.709/2018 (LGPD) ou outras leis internacionais sobre proteção de dados. Por outra linha, aqui, optou-se por utilizar de contornos decorrentes do próprio direito fundamental à proteção de dados (*v.g.*, autodeterminação informativa, dimensões subjetiva e objetiva e seus princípios) para o exame selecionado. Nessa medida, entende-se pela essencial relevância deste método, eis que apresenta a possibilidade de se ter um parâmetro de estatura constitucional para impugnação de atos contrários à proteção de dados pessoais.

Ainda, cumpre destacar que a escolha da Alemanha como a principal fonte de pesquisa no direito internacional se dá em razão do estado da matéria neste país. É que, ao lado dos Estados Unidos da América (conforme destacado na introdução), essa nação se configurara como pioneira da regulação da privacidade e da proteção de dados, desde a concepção até o amadurecimento jurídico do tema. Entre outros pontos, a doutrina coloca como razão para esse

[18] Sobre a questão: "O Poder Judiciário, a quem incumbe inclusive o controle do cumprimento dos deveres de proteção pelos demais órgãos estatais (tanto no nível da proibição do excesso de intervenção quanto no da insuficiência de proteção), já contribuiu e tem contribuído em diversos aspectos, como, por exemplo, ao reconhecer um direito fundamental à proteção de dados e um direito à autodeterminação informativa, ainda que se possa afirmar que se trata de institutos (ainda – em parte) carentes de maior delimitação e desenvolvimento dogmático, em especial na própria seara jurisdicional, mas também doutrinário-acadêmica, nada obstante a existência já de relevantes estudos sobre o tema no Brasil". SARLET, Ingo Wolfgang. **Fundamentos constitucionais**: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 50.

vanguardismo o fato de essas regiões desenvolverem-se econômica e tecnologicamente mais cedo. Assim, houve provocações para discutir e regular os problemas ligados à privacidade e à proteção de dados, emanando dos dois países as principais lições sobre essas matérias[19].

Ademais, o presente trabalho busca apresentar a doutrina nacional e estrangeira mais atualizada sobre o tema, esforço despendido por meio de uma ampla revisão bibliográfica. Já a jurisprudência considerada mais emblemática e importante sobre as questões levantadas será exposta na monografia mediante detalhada análise documental. Sobre esse ponto, destaca-se que as seleções desses julgados foram desenvolvidas a partir do impacto das decisões no entendimento e aplicação da matéria, verificação que foi retirada da doutrina mais especializada.

[19] DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 5.

CAPÍTULO I: A CONSTITUCIONALIZAÇÃO DA PROTEÇÃO DE DADOS NO DIREITO ALEMÃO

Estudo a partir de uma análise jurisprudencial do Tribunal Constitucional Federal alemão

Seguramente, o direito alemão consiste em um dos berços do direito à proteção de dados pessoais, tanto em seu desenvolvimento infraconstitucional como em seu aspecto constitucional. Assim sendo e a alinhado às finalidades deste trabalho, o capítulo presente incumbir-se-á de expor o que há de mais essencial nas lições germânicas sobre a formulação constitucional da tutela de dados pessoais.

Para tanto, optou-se por apresentar relevantes decisões do Tribunal Constitucional Federal alemão e, a partir delas, expor contornos centrais do direito fundamental à proteção de dados pessoais, oriundos da doutrina e/ou da própria Corte Constitucional alemã. Assim, em primeiro, serão apresentadas construções jurisprudenciais sobre o direito geral da personalidade, bem como sua importância para a origem do direito fundamental à proteção de dados. Em segundo, é vez de analisar a famosa decisão sobre o censo demográfico de 1983, aliando tal estudo aos princípios gerais da proteção de dados. Por fim, vale destaque a decisão que reconheceu o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais e sua correlação com as dimensões objetiva e subjetiva do direito fundamental à proteção de dados.

1.1. A CONSTRUÇÃO DO DIREITO GERAL DA PERSONALIDADE NO DIREITO ALEMÃO:

O direito alemão tem importância ímpar para o desenvolvimento do tratamento jurídico acerca da proteção de dados e, nesse contexto, importante demonstrar o desenvolvimento da principal base teórica dessa garantia, qual seja, o direito geral da personalidade. Foi em decisão[20] de 1954, tomada pelo *Bundesgerichtshof* (BGHZ), o Tribunal de Justiça Federal alemão, que se reconheceu o direito geral da personalidade como garantia autônoma[21].

Na ocasião, o Tribunal debruçou-se ante demanda que versava sobre o pedido de um advogado que pretendia corrigir uma nota sua publicada em um meio de comunicação, alegando

[20] BGHZ 13, 334.

[21] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, p. 45, jul-ago 2015.

que caberia somente a ele mesmo decidir se e como suas palavras seriam disponibilizadas ao público. Nesse contexto, considerando que as palavras associadas a um indivíduo é uma clara forma de projeção de sua personalidade, com repercussão direta na sua vida, o Tribunal entendeu pelo provimento da ação. O escopo argumentativo teórico fundou-se exatamente no direito geral da personalidade, garantia constitucional construída em decorrência direta da dignidade da pessoa humana (art. 1º da Lei Fundamental alemã) e do livre desenvolvimento da personalidade (art. 2º da Lei Fundamental alemã)[22].

Com o tempo, a discussão desenvolveu-se no âmbito do Tribunal Constitucional Federal alemão, o *Bundesverfassungsgerichts* (BVerfG), bem como passou a ser objeto de forte interesse pela doutrina. Nesse viés, ficou entendido que a interpretação conjunta da dignidade da pessoa humana e do livre desenvolvimento da personalidade resultam, de um lado, na liberdade geral de ação[23] e, por outro lado, no direito geral da personalidade, o qual se passa a analisar.

O direito geral da personalidade busca tutelar os elementos vinculados a personalidade como um todo. Dessa forma, em sua dogmática, separaram-se três eixos principais, quais sejam: (i) o direito à autodeterminação, que diz respeito à prerrogativa de o cidadão determinar sua identidade, seu destino (*v.g.*, orientação sexual, ter filhos ou não); (ii) o direito à autoconservação ou autopreservação, consistente no direito de ficar só, de não dividir questões pessoais com a dimensão externa (*v.g.*, sigilo de um diário pessoal, confidencialidade de questões médicas); e (iii) o direito à auto-exposição ou auto-apresentação, que se traduz na garantia que cada indivíduo tem de optar pela forma como se apresentará ao mundo, cabendo-

[22] Na mencionada decisão, colocou-se: ”Além disso, agora que a Lei Básica [Constituição de 1949] reconheceu o direito do ser humano a ter sua dignidade respeitada (Art. 1), e também o direito ao livre desenvolvimento de sua personalidade como um direito privado, a ser universalmente respeitado na medida em que não viole o direito alheio ou não esteja em conflito com a ordem constitucional ou a moral (art. 2º), o direito geral da personalidade deve ser considerado um direito fundamental garantido constitucionalmente.” BGHZ 13, 334. (tradução livre de: ”Nachdem nunmehr das Grundgesetz das Recht des Menschen auf Achtung seiner Würde (Art. 1 GrundG) und das Recht auf freie Entfaltung seiner Persönlichkeit auch als privates, von jedermann zu achtendes Recht anerkennt, soweit dieses Recht nicht die Rechte anderer verletzt oder gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt (Art. 2 GrundG) muß das allgemeine Persönlichkeitsrecht als ein verfassungsmäßig gewährleistetes Grundrecht angesehen werden.”
No mesmo sentido: ”o Tribunal Federal de Justiça (BGH – Bundesgerichtshof) desenvolveu um direito geral da personalidade (allgemeines Persönlichkeitsrecht), definindo-o como um direito do indivíduo ao respeito de sua dignidade humana e de desenvolvimento de sua personalidade individual (Recht auf freie Entfaltung der Persönlichkeit). Assim sendo, o direito geral da personalidade derivou do conceito de dignidade da pessoa humana (art. 1º da Lei Fundamental) e do direito ao livre desenvolvimento da personalidade (art. 2º da Lei Fundamental). Foi reconhecido como um direito constitucionalmente garantido pela primeira vez no ano de 1954, com a célebre decisão do caso Leserbrief” ZANINI, Leonardo Estevam de Assis. A proteção dos direitos da personalidade na Alemanha. **Revista Direitos Culturais**, Santo Ângelo-RS, v. 14, n. 33, p. 140, 2019.

[23] vide BVerfGE 6, 32 – *Elfes*

lhe opor-se às informações falsas ou secretas sobre ele (*v.g.*, direito à honra e imagem)[24]. Aliás, é sobre o escopo desse último eixo que se desenvolveu o direito à autodeterminação informativa, como será exposto no próximo tópico do trabalho.

No âmbito jurisprudencial, decisão *Tonband* de 1973[25] foi de significativa importância para a consolidação do direito geral da personalidade. No caso, um casal vendeu um apartamento no valor de 495.000 marcos alemães, sendo, todavia, apenas 425.000 marcos registrados na escritura, com os 70.000 marcos restantes transferidos mediante assinatura de recibo de empréstimo, que deveria ser destruído no momento da transferência do imóvel. Anos depois, contudo, o comprador cobrou o valor do empréstimo, sendo acusado de estelionato pelo casal, que fundou as provas em gravação de fita fonográfica de conversa que atestava o acordo verbal entre as partes, mesmo sem o conhecimento e consentimento do comprador. Inconformado com decisões da primeira instância que o julgaram culpado, o acusado de estelionato ingressou com ação constitucional questionando a legitimidade da prova.

Frente a essa contenda, o Tribunal Constitucional Federal alemão afirmou as bases do direito geral da personalidade, colocando-o como consequência da dignidade da pessoa humana e o livre desenvolvimento da personalidade, localizados, respectivamente, no art. 1º e 2º, da Constituição Alemã. Ademais, consignou sobre a importância do princípio da proporcionalidade, através do qual se pode limitar o direito geral da personalidade em nome de um interesse superior. Todavia, no caso concreto, a Corte entendeu que, dada a ponderação de valores na situação, não justificaria a intervenção no direito geral da personalidade do acusado[26], ponderando que a gravação feita sem consentimento foi uma grave intervenção sem um interesse preponderante da coletividade à altura.

---

[24] SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, pp. 189-190. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 27/05/2021. MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira - RJLB**, Ano 5, nº 1, p. 787, 2019.

[25] BVerfGE 34, 238 – *Tonband*. Traduzida em: SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, pp. 195-198. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 27/05/2021.

[26] Nesse sentido: ”O direito constitucionalmente garantido ao livre desenvolvimento da personalidade e as condições de uma jurisdição eficiente podem entrar em conflito de variadas formas. Pode-se conseguir um equilíbrio justo destas tensões somente quando, como corretivo, sempre for contraposto às intervenções necessárias para uma jurisdição eficiente o mandamento de proteção do Art. 2 I c.c. Art. 1 I GG (cf. BVerfGE 19, 342 [347]; 20, 45 [49], 144 [147]). Isso significa que deve ser averiguado a qual desses importantes princípios constitucionais deve ser atribuído maior peso em cada caso particular”. Decisão traduzida em: SCHWABE, Jürgen; MARTINS, Leonardo. Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Montevideo: Konrad Adenauer Stiftung, 2005, p. 198. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 27/05/2021.

Nesse aspecto, resta claro uma das principais características do direito geral da personalidade, qual seja, a sua aplicabilidade em casos em que há ausência de uma proteção específica da personalidade. É o que Gernit Hornung e Cristoph Schnabel chamam de "função de fechamento de lacunas do direito geral da personalidade"[27]. No mesmo sentido, consigna Karl Larenz, afirmando que tal garantia é um direito fonte (*Quellrecht*), donde abre-se espaço para que se derivem várias proteções específicas relativas à personalidade[28]. É dizer: o direito geral da personalidade tem função ímpar de atualizar a tutela da personalidade humana, tendo em vista que as circunstâncias gerais e eventuais novos riscos para a personalidade estão inseridos em um processo dinâmico, o que impossibilita uma assimilação instantânea do direito.

O Tribunal Constitucional Federal alemão sempre esteve atento a essa problemática e, à exemplo da decisão *Tonband* supracitada, já se utilizou do direito geral da personalidade inúmeras vezes. Aliás, vez que a Corte Constitucional alemã deixou clara essa função de fechamento de lacunas foi na decisão *Scientology*[29], que tratou de conflito normativo entre o direito geral da personalidade e a liberdade de expressão. Na oportunidade, restou esposada com clareza a ampla função de cobrir lacunas desse direito: "O direito fundamental protege elementos da personalidade que não são objeto de garantias especiais de liberdade, mas que não são menos importantes para a personalidade em seu significado constitutivo"[30].

Outro aspecto central na aplicação do direito geral da personalidade diz respeito ao princípio da proporcionalidade – como mencionado na decisão *Tonband*. Sobre a questão, Zanini[31] afirma que a elasticidade na aplicação desse direito impõe mais restrições a sua aplicação, o que vai depender sempre da análise das circunstâncias na pretensão posta. É dizer: são recorrentes a concorrência de outros interesses jurídicos relevantes com o direito geral da personalidade, o que resulta na necessidade de evocar o princípio da proporcionalidade para que, caso a caso, pondere-se qual valor jurídico deve prevalecer[32].

---

[27] tradução livre de: ''gapclosing function of the general personality right" HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. **Computer Law And Security Review**, Kassel, n. 25, p.115-122, 2009.

[28] Vide citação sobre a obra "LARENZ, Karl. Allgemeiner Teil des Bürgerlichen Rechts, p. 128" na página 141 de "ZANINI, Leonardo Estevam de Assis. A proteção dos direitos da personalidade na Alemanha. Revista Direitos Culturais, Santo Ângelo-RS, v. 14, n. 33, p. 135-158, 2019."

[29] BVerfGE 99, 185 – *Scientology*. Traduzida em: SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005, pp. 198-207. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 27/05/2021.

[30] *Ibidem.* pp. 201-202.

[31] ZANINI, Leonardo Estevam de Assis. A proteção dos direitos da personalidade na Alemanha. **Revista Direitos Culturais**, Santo Ângelo-RS, v. 14, n. 33, p. 141, 2019.

[32] A importância do princípio da proporcionalidade é generalizada na hermenêutica constitucional. Não é diferente para fins do direito fundamental à proteção de dados, que decorre, em parte, do próprio direito geral da

Por fim, impende destacar o que levou o Tribunal Constitucional Federal alemão ao reconhecimento do direito à autodeterminação informativa – próximo passo a ser analisado neste trabalho. Destaca-se, nesse sentido, a teoria das esferas da personalidade ou teoria do núcleo da personalidade[33], que tinha forte respaldo doutrinário e jurisprudencial na Alemanha. A ideia era a de que a proporcionalidade se dividia em três esferas distintas: a íntima, a privada e a social, cada qual merecedora de proteção diferenciada.

Todavia, com o desenvolvimento da tecnologia, sobretudo das modernas ferramentas de processamento de dados na década de 1980, viu-se tal escala de proteção como ferramenta antiquada. É que os dados pessoais, independente da informação que carregavam consigo, passaram a representar graves riscos em face das diversas possibilidades decorrentes do processamento automatizado[34]. Portanto, far-se-ia necessário o reconhecimento de um direito autônomo de tutela dos dados pessoais, o que veio a acontecer em 1983, com a emblemática decisão que se passa a analisar.

1.2. A DECISÃO DE 1983 SOBRE A LEI DO CENSO (*VOLKSZÄHLUNGSURTEIL*) E OS PRINCÍPIOS GERAIS DA PROTEÇÃO DE DADOS:

A Lei do Censo (*Volkszählungsgesetz*), de 25 de março de 1982, estabeleceu que deveria ser feito um recenseamento geral no início de 1983. Para tanto, mediante 160 perguntas que gerariam dados para tratamento informatizados[35], seriam recolhidas informações acerca da profissão, moradia e local de trabalho dos cidadãos. Segundo o próprio texto normativo, o objetivo dos Censo consistia em analisar o estágio do crescimento populacional, sua distribuição espacial e atividade econômica. Ademais, segundo o § 9 do diploma normativo, os

personalidade. Assim sendo, será de extrema relevância para o recorte de pesquisa deste trabalho a apresentação de métodos de verificação da proporcionalidade, como o proposto por Gillian Black e Leslie Stevens.

[33] Tal teoria foi defendida em diversas obras, tal qual: Peters, Das Recht der freien Entfaltung der Persönlichkeit in der höchstrichterlichen Rechtsprechung, 1963.

[34] Baseando-se em Leonardo Martins (MARTINS, Leonardo. Die Grundrechtskollision. Grundrechtskonkretisierung am Beispiel des 41 1 BDSG. Berlim: Humbold-Universitat zu Berlin, 2001), Jhonata Assmann afirma: "A jurisprudência baseada na teoria das esferas, até o advento da Volkszahlungsurteil majoritária no TCF, revelou-se, no entanto, insuficiente (...). Para a questão da proteção de dados, as limitações da teoria das esferas afiguram-se ainda mais notáveis. A utilização da teoria das esferas significa que nem toda informação privada precisa ser protegida, senão apenas aquelas que possam ser consideradas da esfera íntima." ASSMANN, JHONATA. **O Direito à Autodeterminação Informativa no Direito Germânico e Brasileiro.** Orientador: Airton Lisle Cerqueira L. Seelaender. 2014. 65 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: http://150.162.242.35/bitstream/handle/123456789/117169/Jhonata%20Assmann%20TCC%20pdfa.pdf?sequence=1&isAllowed=y. Acesso em: 02 jun. 2021.

[35] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Renovar, 2006. p. 193.

dados estariam disponíveis para a comparação com as informações do registro público, bem como para o compartilhamento com outros órgãos do poder público para fins específicos de execução administrativa.

Diante da imposição normativa, ascendeu-se debate na sociedade civil e Reclamações Constitucionais foram ajuizadas, culminando no histórico julgamento do Tribunal Constitucional Federal alemão, em 15 de dezembro de 1983. Na ocasião, confirmou-se a constitucionalidade da lei, contudo, alguns dispositivos, principalmente sobre a transferência de dados entre os órgãos públicos e sobre a possibilidade de comparação de dados, foram declarados inconstitucionais.

Antes de adentrar na decisão em si, cumpre destacar seus principais êxitos, quais sejam: (i) o concebimento do direito à autodeterminação informativa, que, ao reconhecer um direito fundamental subjetivo, estruturou um marco teórico para o desenvolvimento do direito à proteção de dados e elevou o indivíduo a protagonista da proteção de dados[36]; e (ii) a desmistificação do entendimento de que há dados irrelevantes, segundo o veredito, dados aparentemente inofensivos podem adquirir novos valores a partir do processamento automático[37].

Destaca-se, aliás, que tamanha é a importância dessa decisão a ponto de ser interpretada como marco para a terceira geração de normas sobre proteção de dados, da divisão geracional formulada por Viktor Mayer-Schönberger[38]. Nesse contexto, é ressaltado que o decidido pela Corte Constitucional alemã teve grande repercussão na edição de diversas legislações, sobretudo na criação de mecanismos de empoderamento da participação do titular no tratamento de seus dados.

Adentrando no mérito da contenda, é possível realizar divisão da decisão em quatro partes: (i) o panorama tecnológico e o direito à autodeterminação informativa; (ii) os limites do direito à autodeterminação informativa; (iii) a distinção entre dados processados individualmente e dados para fins estatísticos; e (iv) conclusões.

Sobre o primeiro ponto, a decisão começa ponderando acerca de valores constitucionais centrais, quais sejam, a dignidade da pessoa humana e direito geral da personalidade. Nesse sentido, destaca-se que o direito da personalidade ganha expressiva importância na proteção da

---

[36] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.** São Paulo: Saraiva, 2014. p. 31.

[37] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Renovar, 2006. p. 195.

[38] MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and privacy: the new landscape.** Cambridge: The Mit Press, 1997.

dignidade da pessoa humana em face do desenvolvimento tecnológico, o processamento automático de dados e as consequentes ameaças ao livre desenvolvimento da personalidade. É desse contexto que emerge o direito à autodeterminação informativa, que determina o poder do indivíduo "de decidir em princípio por si próprio, quando e dentro de que limites fatos pessoais serão revelados"[39].

Nesse diapasão, é de suma importância verificar que a própria decisão foi além da identificação apenas de uma dimensão de importância predominantemente individual (desenvolvimento da personalidade). Em vez disso, o Tribunal alemão também fundou as bases da importância do direito à autodeterminação informativa em uma dimensão democrática e de interesse público. É dizer: o fato de as pessoas não terem com clareza quais dados sobre elas são conhecidos mina significantemente sua liberdade de agir e se expressar, por exemplo, o fato de a participação de um cidadão em uma reunião ou manifestação ser registrada pode desencorajar sua participação, configurando um óbice para além do mero desenvolvimento da individualidade, mas que alcança o próprio bem comum e as premissas de um Estado Democrático[40].

---

[39] SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Decisão do Tribunal Constitucional alemão de 1983. Montevideo: Konrad Adenauer Stiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. p. 237.

[40] Nesse sentido: "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 com uma ordem jurídica que possibilite que os cidadãos não possam mais saber quem sabe o que sobre eles, quando e em que ocasião. Qualquer pessoa que não tenha certeza se um comportamento divergente é observado a qualquer momento e permanentemente armazenado, usado ou repassado como informação, tentará não chamar a atenção por meio de tal comportamento. Quem está esperando que, por exemplo, a participação em uma reunião ou uma iniciativa de cidadania esteja oficialmente registrada e que daí possam surgir riscos, possivelmente se absterá de exercer seus correspondentes direitos básicos (Art. 8, 9 GG). Isso prejudicaria não apenas as chances de desenvolvimento do indivíduo, mas também o bem comum, pois a autodeterminação é uma condição funcional elementar de uma comunidade democrática livre baseada na capacidade de agir e participar de seus cidadãos." (tradução livre: "Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.") BVerfGE 65, 1, 154 – *Volkszahlung*

Todavia, em segundo lugar, a decisão destaca que tal direito não pode ser absoluto e ilimitado. O cidadão, enquanto ser dependente da comunicação para a inserção na comunidade social, deve aceitar limitações ao direito à autodeterminação. Dessa forma, tendo em vista o princípio da proporcionalidade, deve-se sempre realizar uma ponderação de equilíbrio entre esse direito e outros interesses constitucionais[41].

O terceiro ponto trata da diferenciação entre o tratamento de dados pessoais não anônimos e dados para fins estatísticos. Como premissa, cabe destaque ponto crucial da decisão já mencionado: diante do estado da arte da tecnologia e do processamento de dados na época, concluiu-se que não há dados que sejam irrelevantes. É que informações aparentemente insignificantes, a partir de um tratamento de dados, têm potencial de adquirir novos valores e serem ofensivas aos direitos da personalidade do cidadão.

Assim sendo, é regra que dados não anônimos devem ser tratados de acordo com a vontade, conhecimento e possibilidade de intervenção do titular. Mesmo que, em muitos casos, mostra-se essencial a limitação da autodeterminação informativa para o tratamento de dados pessoais associáveis ao titular, especialmente quando for para cumprir uma função administrativa, como a concessão de benefícios sociais. Destaca-se, nesse ínterim, a necessidade da observância do princípio da proporcionalidade para o estabelecimento de medidas que protejam o indivíduo, das quais ressaltam-se: a vinculação do uso do dado a sua finalidade, o dimensionamento mínimo necessário do dado para o seu fim e transparência com o titular dos dados[42].

Por outro lado, é dada solução diferente para o levantamento de dados para fins estatísticos. Em face da importância desta atividade para a política governamental no contexto do Estado Social e sua própria essência, afasta-se a necessidade de vinculação de dados aos seus fins. Isto é, quando para fins estatísticos, os dados podem ser armazenados para as mais diversas tarefas, não devendo, de antemão, ter suas destinações estabelecidas. Todavia, essa maior liberdade para tratamento de dados requer que sejam impostos limites compensatórios. Assim, a decisão determina a necessidade de que os dados sejam usados apenas para ajudar em tarefas públicas e, principalmente, de que os dados sejam tornados anônimos o mais rápido possível e, enquanto assim não o for, respeitar sigilo absoluto sobre as informações[43].

Por fim, a parte dispositiva da decisão declara a constitucionalidade geral da Lei do Recenseamento, com a ressalva de que seja feita regulamentação acerca da organização e

[41] *Ibidem.* pp. 238-239.
[42] *Ibidem.* pp. 239-241.
[43] *Ibidem.* pp. 241-244.

procedimento do censo. Todavia, as partes relativas à possibilidade de comparação dos dados obtidos com o registro público e à transmissão de dados para fins de execução administrativa foram compreendidas como ofensas ao direito da personalidade e, portanto, declaradas inconstitucionais. Ocorre que, na realidade, uma nova lei foi promulgada em 1985, sendo o censo realizado em 1987, sob a égide de regras compatíveis com a decisão[44].

Dado o contexto e fundamentos da *Volkszählungsurteil*, merece atenção especial para os fins deste trabalho o arcabouço principiológico referente à proteção de dados[45]. A título de exemplo, quando na própria decisão, determinou-se que em casos de tratamento de dados para objetivos estatísticos pode-se flexibilizar a condição de se vincular o tratamento aos seus fins, falou-se em um dos princípios gerais da proteção de dados: o da finalidade. Daí depreende que, em que pese o hábito de se conceituar e consolidar tais princípios nas modernas leis de proteção de dados, esses decorrem da própria garantia fundamental, isto é, têm valor constitucional.

É bem verdade que a construção desses princípios não tem gênese exclusiva no território alemão. Como Laura Mendes e Bruno Bioni afirmam, os princípios gerais da proteção de dados nasceram praticamente de modo simultâneo nos EUA, Inglaterra e Alemanha, desenvolvendo um rol de diretrizes que encontram resguardo, de forma quase sempre igual, nos diferentes sistemas jurídicos do mundo[46].

Levando em conta as raras variações entre os diplomas jurídicos, vale aqui destacar alguns dos princípios gerais elementares da proteção de dados – sem pretensão exauriente – que serão úteis para a própria análise de constitucionalidade do diploma normativo selecionado, no

---

[44] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Renovar, 2006. p. 196.

[45] Sobre a diferenciação do direito fundamental à proteção de dados e a autodeterminação informativa, é de grande valia colacionar lição de Ingo Wolfgang, na qual depreende-se que este é parte daquele, senão vejamos: "Ainda em sede preliminar, é de se observar que, nada obstante a circunstância de que o direito à proteção de dados pessoais guarda relação direta (mas, como já adiantado, não se confunde) com um direito à autodeterminação informativa – que, de todo modo, é um dos esteios e elementos centrais da proteção de dados – na sua condição de direito subjetivo, o catálogo de posições jusfundamentais que encerra é bastante diversificado." SARLET, Ingo Wolfgang. **Fundamentos constitucionais**: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 21-61.

[46] MENDES, Laura Schertel; BIONI, Bruno. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor.** Vol. 124. Ano 28. São Paulo: Editora RT, p. 166, jul-ago 2019.

Nos **Estados Unidos da América**, a formulação dos princípios ficou a cargo do *Department of Health, Education, and Welfare*, que emitiu relatório em 1973 com a definição do conceito de privacidade, bem como a proposição de cinco princípios basilares que deveriam guiar o tratamento de dados.

Na mesma época, a **Grã-Bretanha**, mediante o criado Comitê de Privacidade, lançou relatório que apresentava preocupação com os riscos gerados pelo tratamento de dados pessoais, sugerindo 10 princípios básicos que visavam a proteção da privacidade.

Por fim, em 1975, na **Alemanha**, foi editada a primeira legislação que regulava a proteção de dados – Lei do Estado de Hesse –, contendo arcabouço principiológico muito similar aos dos documentos estadunidense e inglês.

terceiro capítulo. Passe-se a breve análise, então, dos seguintes princípios: (i) finalidade; (ii) adequação; (iii) necessidade; (iv) transparência da informação; e (v) segurança da informação[47].

O princípio da finalidade traduz-se na obrigação de o tratamento ser guiado por fins legítimos, específicos, explícitos e informados. O princípio da adequação pode ser visto como uma consequência direta do da finalidade, na medida em que exige a compatibilidade contínua do tratamento com a finalidade para qual os dados foram coletados. Já o princípio da necessidade preceitua que os dados coletados devem ser os mínimos necessários para a realização da finalidade proposta, isto é, deve haver proporcionalidade entre a abrangência dos dados coletados e as finalidades pretendidas. Por sua vez, o princípio da transparência consiste na regra de a existência dos bancos de dados serem de conhecimento público, bem como na garantia de os titulares obterem informações claras e precisas sobre o tratamento de seus dados. Por último, tem-se o princípio da segurança da informação, traduzido na necessidade de utilizar-se de medidas técnicas e administrativas que previnam contra a violação dos dados tratados.

1.3. DIREITO FUNDAMENTAL À GARANTIA DA CONFIDENCIALIDADE E DA INTEGRIDADE DOS SISTEMAS TÉCNICO-INFORMACIONAIS E AS DIMENSÕES DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS:

É bem verdade que o estado da tecnologia sofreu intensas mudanças desde que se proferiu o acórdão em 1983 até o século XXI. Sobre esse desenvolvimento, destaca-se a "digitalización, miniaturización, conexión en red, desarrollo de nuevas infraestructuras y creación de nuevos servicios (en particular sociales)"[48], com um destaque especial para o advento da utilização generalizada da rede mundial de computadores (*Internet*).

Tal contexto permitiu que se abrissem diversas novas oportunidades para a sociedade moderna, que passou a transferir importantes aspectos da vida para os meios digitais, seja para os fins de armazenamento em nuvens, para as comunicações privados ou para as interações em

[47] vide: DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Renovar, 2006. pp. 216-217.
BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Art. 6º. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03 jun. 2021.
[48] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, p. 48, jul-ago 2015.

redes sociais. De qualquer forma, constata-se que os meios técnico-informacionais ganharam configurações de verdadeiros *locus* de desenvolvimento da personalidade humana.

Nesse contexto, os dados pessoais oriundos dessa nova dinâmica tecnológica tornaram-se base para a consecução de diversos objetivos, incluindo uma série de modelos de negócios, que moldam os desenvolvimentos econômicos e sociais modernos. Todavia, como já visto neste trabalho, o alargamento de possibilidades tecnológicas e a utilização generalizada dos dados decorrentes dessas inovações representam um sério risco para os direitos fundamentais do cidadão. Um exemplo disso é o monitoramento de sistemas técnico-informacionais, como celulares e notebooks, pelos órgãos de segurança pública, questão sobre a qual o Tribunal Constitucional Federal alemão foi provocado a debruçar-se[49].

Como premissa, deve-se compreender que, paralelamente à facilidade comunicativa gerada pelos novos softwares de comunicação (*v.g., Whatsapp, Telegram, Skype*), na sociedade como um todo, tornou-se mais elementar também o uso dessas tecnologias por delinquentes, com objetivos criminosos. Ocorre que mecanismos típicos desses aplicativos, tal qual a criptografia ponta a ponta, fazem com que a vigilância seja mais difícil do que em outrora. Exemplo disso é que se mostra impossível a coleta de informações durante o processo comunicativo como ocorria na via telefônica. Na verdade, faz-se necessário invadir o sistema técnico-informacional antes do processo comunicativo, o que se executa com auxílio de *malwares*, como o cavalo de Troia[50].

Nesse sentido, dispositivos da lei regional da Renânia do Norte-Vestifália, que visavam a proteção da Constituição Estadual, regulamentaram acerca da possibilidade de invasão e o monitoramento remoto de sistemas de tecnologia da informação de suspeitos de cometer ilícitos penais, o que se daria mediante simples autorização de autoridade administrativa[51]. Assim

---

[49] BVerfGE 120, 274 - *Online-Durchsuchungen*

[50] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, p. 48, jul-ago 2015. Segundo Hoffmann-Riem, essa foi exatamente o questionamento que chegou a Suprema Corte alemã. Em suas palavras: "¿Tiene derecho el Estado a infiltrarse en ordenadores privados – o dicho en términos más amplios, en sistemas privados de tratamiento de la información – mediante el correspondiente software, los llamados troyanos, con el fin de recoger y utilizar de modo secreto datos personales, tanto operativos como de contenido? " *Ibidem.* p. 51.

[51] Como bem expõe Fabiano Menke, uma real atenção foi colocada sobre a lei apenas após a proposição de transposição para o nível federal: "Apesar de a mencionada lei não ter chamado muito a atenção logo após ser editada, passou a ser foco de intensa discussão a partir do momento em que o ministro de Estado Wolfgang Schäuble resolveu propor, em nível federal, a adoção dos mesmos dispositivos que autorizavam o monitoramento remoto de computadores de suspeitos da lei de Nordrhein-Westfalen." MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira – RJLB**, Ano 5, nº 1, p. 794, 2019.

sendo, tais disposições foram objeto de reclamação constitucional em razão de suposta violação ao direito da personalidade e à dignidade da pessoa humana, contenda decidida pelo Tribunal Constitucional Federal alemão em 2008.

Na oportunidade, lançando mão do princípio da proporcionalidade, o Tribunal entendeu que os critérios presentes no diploma normativo eram insuficientes para justificar a invasão prevista, reconhecendo, nesse sentido, um novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais. Vale frisar que, a par do método utilizado pela Corte alemã no reconhecimento da autodeterminação informativa, o percurso hermenêutico para o reconhecimento da nova garantia mencionada deu-se a partir do direito geral da personalidade e sua função de preencher lacunas[52].

Pelo exposto, como afirma com precisão Rainer Erd[53], professor da Universidade de Frankfurt, o direito à garantia da confidencialidade e integridade dos sistemas técnico-informacionais figura como mecanismo de proteção da personalidade atualizada à conjuntura tecnológica do século XXI. Nesse viés, faz-se relevante mostrar a necessidade desta nova garantia, sobretudo apresentando suas diferenças em relação à autodeterminação informativa.

Por um lado, há vozes na doutrina alemã que criticam a formulação desse novo direito, afirmando que tal espaço poderia facilmente ser preenchido e solucionado pela já existente autodeterminação informativa[54]. Em outra perspectiva, há quem defenda como acertada a decisão da Corte alemã em reconhecer a nova garantia, vez que a autodeterminação informativa não conferiria proteção à situação da norma impugnada na reclamação constitucional, isto é, ao contexto no qual "terceiros que acabam tendo acesso a dados armazenados em algum sistema técnico-informático não se encontram sujeitos às regras sobre a coleta e tratamento de tais

---

[52] Nesse sentido, colaciona o seguinte trecho da decisão: "O direito geral de personalidade garante elementos de personalidade que não são objetos das garantias especiais da Lei Fundamental, mas não são inferiores a eles em termos de seu significado constituinte para a personalidade (cf. BVerfGE 99, 185 [193]; 114, 339 [346]). Essa garantia de redução de lacunas é necessária, em particular, para conter novos tipos de ameaças que podem surgir no curso do progresso científico e técnico e mudanças nas condições de vida (cf. BVerfGE 54, 148 [153]; 65, 1 [41]; 118 , 168) [183])." (tradução livre de "Das allgemeine Persönlichkeitsrecht gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen (vgl. BVerfGE 99, 185 [193]; 114, 339 [346]). Einer solchen lückenschließenden Gewährleistung bedarf es insbesondere, um neuartigen Gefährdungen zu begegnen, zu denen es im Zuge des wissenschaftlich-technischen Fortschritts und gewandelter Lebensverhältnisse kommen kann (vgl. BVerfGE 54, 148 [153]; 65, 1 [41]; 118, 168 [183])"). BVerfGE 120, 274, 169.

[53] ERD, Rainer. Bundesverfassungsgericht versus Politik: Eine Kommentierende Dokumentation Der Jüngsten Entscheidungen Zu Drei Sicherheitsgesetzen. **Kritische Justiz**, vol. 41, no. 2, 2008, p. 120. JSTOR, www.jstor.org/stable/24238877. Acesso em 16 jun 2021.

[54] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, p. 53, jul-ago 2015.

dados"[55]. Por isso, os defensores do novo direito fundamental diferenciam as garantias de modo a afirmar que enquanto a autodeterminação informativa protege os dados, ou conjunto de dados, em si, o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais perfaz a tutela do próprio sistema, e dos dados em sentido *lato*[56].

Por fim, a Corte alemã não deixou de estabelecer os limites da nova garantia reconhecida. Assim, tendo em vista que a invasão e monitoramento de sistemas técnico-informacionais representa uma grave e arriscada atividade em relação ao direito da personalidade dos cidadãos, o acórdão prolatado estabeleceu critérios rígidos para que se concretize a exceção, dividindo-os nos seguintes três eixos: (i) necessidade de reserva legal, isto é, a exceção ao novo direito deve-se basear em lei específica, que veicule a hipótese de monitoramento do sistema informático com clareza e em respeito ao princípio da proporcionalidade; (ii) obrigatoriedade de a intervenção se justificar em uma ameaça concreta, que consiste na exposição ao perigo de bem jurídico específico; (iii) exigência de o monitoramento remoto ser outorgado mediante ordem judicial[57].

Noutro giro, cabe trazer à tona relevante reflexão do ex-ministro do Tribunal Constitucional Federal alemão e especialista em proteção de dados, Wolfgang Hoffman-Riem, que ressalta, em análise à decisão aqui examinada, as dimensões subjetiva e objetiva do direito fundamental: importante contorno dogmático do próprio direito fundamental à proteção de dados e, deste modo, relevante para os fins deste trabalho. O jurista, em brilhante artigo[58], sugere que a opção terminológica do termo "garantia" em detrimento do mais usual vocábulo "proteção" representa a pretensão do Tribunal Constitucional Federal alemão de ressaltar, além da mais comum dimensão jurídica-subjetiva do direito reconhecido, a sua dimensão jurídica-objetiva. Tais dimensões são categorizações doutrinárias que se passam a analisar.

---

[55] SARLET, Ingo Wolfgang. **Fundamentos constitucionais**: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 34.

[56] MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira – RJLB**, Ano 5, nº 1, p. 798, 2019.

[57] *Ibidem.* p. 54-57.

[58] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, pp. 54-57, jul-ago 2015.

Por um lado, a dimensão subjetiva dos direitos fundamentais é a que está mais ligada às origens desses direitos, isto é, diz respeitos à garantia de posições individuais, conferindo ao cidadão o direito de exigir determinado comportamento de outrem (negativo ou positivo) ou o poder de produzir efeitos jurídicos em determinadas relações jurídicas. Por outro lado, a dimensão objetiva consiste no valor dos direitos fundamentais como diretrizes da ordem constitucional para todo o funcionamento do Estado Democrático de Direito, ou seja, a essa dimensão faz referência aos direitos fundamentais como a essência de toda atuação do Estado, seja em sua atividade legislativa, jurisdicional ou administrativa[59].

Sobre essas dimensões no que concerne especificamente o direito fundamental à proteção de dados, com base na doutrina alemã[60], a professora Laura Schertel Mendes[61] leciona que a dimensão subjetiva do direito fundamental à proteção de dados consiste em um direito de defesa do cidadão frente possíveis intervenções em sua liberdade e privacidade, ensejando ao indivíduo a pretensão de se opor a atos que violem o seu direito à proteção de dados, bem como de se precaver, exigindo medidas preventivas contra violações a esse direito. A principal manifestação dessa dimensão é a própria autodeterminação informativa, que consiste, sinteticamente, no controle que os cidadãos devem ter de seus dados pessoais.

Já em relação à dimensão objetiva, o acadêmico Ingo Wolfgang, sob a premissa segunda a qual essa dimensão diz respeito à ideia "de que a proteção dos direitos fundamentais depende de estruturas organizacionais e de procedimentos adequados"[62], compreende que tal dimensão é particularmente importante para a uma real garantia da proteção de dados. É que, em face da veloz e constante evolução tecnológica, sobretudo as de informação e comunicação, são ainda mais relevantes as ferramentas voltadas para a prevenção e repressão às violações. Sobre essas ferramentas, destaca-se extenso rol de possibilidades, que vão desde a criação de sanções penais e administrativas até a criação e estruturação de eficientes órgãos públicos ou privados, tal qual

---

[59] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** São Paulo: Editora Saraiva, 2018, pp. 168-170.

[60] *Verbi gratia*, PIEROTH, Bodo; SCHLINK, Bernhard. **Grundrechte – Staatsrechte II**. Heidelberg: Müller Verlag, 2005; GRIMM, Dieter. Persönlichkeitsschutz im Verfassungsrecht. **Karlsruher Forum 1996. Schutz der Persönlichkeit. Mit Vorträgen von Dieter Grimm und Peter Scherdtner**. Karlsruhe: Versicherungswirtschaft, 1997.

[61] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 205-206, jul./dez. 2018.

[62] SARLET, Ingo Wolfgang. **Fundamentos constitucionais**: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, p. 46.

a Autoridade Nacional de Proteção de Dados, prevista nos arts. 55-A a 55-L, da Lei nº 13.709/2018 - LGPD[63].

Nesse sentido, como bem pontua Laura Schertel Mendes, a dimensão objetiva desse direito fundamental implica na irradiação dessa garantia para todo ordenamento jurídico, de modo que, como primeiro destinatário, configura tarefa obrigatória do legislador em sua atividade o respeito aos preceitos emanados dessa garantia fundamental. Em segundo, como destinatário subsidiário, resta como obrigação do Estado-Juiz a aplicação do direito fundamental, quando, em face da insuficiência ou ofensa dos atos do legislativo ao direito fundamental, o judiciário deve resguardar a proteção de dados a partir de normas já reconhecidas[64].

Dado todo o exposto acerca da construção do direito fundamental à proteção de dados em um de seus principais berços, bem como a exposição do que se julgou ser os desenvolvimentos dogmáticos mais relevantes dessa garantia, passa-se, no próximo capítulo, a análise minuciosa de como o mesmo tema é tratado no contexto brasileiro, com enfoque nos desenvolvimentos doutrinários e nos entendimentos jurisprudenciais.

---

[63] *Ibidem.* p. 44-47.

[64] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 208-209, jul./dez. 2018. Na página 209 do mesmo texto, afirma a Professora que ”[n] esse sentido, configura-se a violação ao direito fundamental não apenas com a indevida intervenção do Estado na esfera privada, mas principalmente, com a não atuação ou atuação insuficiente estatal para garantir a proteção do cidadão contra os riscos à personalidade causados pelo tratamento de dados pessoais.”.

CAPÍTULO II: A PROTEÇÃO DE DADOS E O PANORAMA CONSTITUCIONAL BRASILEIRO

As disposições constitucionais e suas interpretações no Brasil

Este segundo capítulo está dividido em duas partes que buscam analisar o desenvolvimento constitucional da proteção de dados no contexto brasileiro.

Na primeira, busca-se minuciar um panorama da doutrina acerca do entendimento constitucional da proteção de dados na atividade estatal, ressaltando a interpretação dos dispositivos constitucionais que tangenciam o tema, a discussão sobre um direito autônomo à proteção de dados e a Proposta de Emenda à Constituição nº 17/2019 – que visa fixar a garantia de forma expressa na Constituição Federal. Por sua vez, a segunda parte cuida de apresentar o que se entende por mais relevante entre os precedentes do Supremo Tribunal Federal sobre o tema, sendo manifesta uma clara evolução interpretativa na Corte que culminou no recentíssimo reconhecimento de um direito fundamental à proteção de dados.

2.1. O CAMINHO ATÉ O RECONHECIMENTO DE UM DIREITO FUNDAMENTAL AUTÔNOMO À PROTEÇÃO DE DADOS NA DOUTRINA BRASILEIRA:

Como exposto na introdução, no contexto internacional, a matéria da proteção de dados ganhou qualificação legal na década de 1970 e, apenas nos limiares da década seguinte, conquistou estatura constitucional, sobretudo com a decisão do Tribunal Constitucional Federal da Alemanha sobre o recenseamento, em 1983, e com a Convenção nº 181[65], da União Europeia, em 1981. Todavia, essa consolidação não foi absorvida de maneira uniforme em todo mundo. Deveras, ainda no século XXI, observa-se que vários Estados Constitucionais ainda não reconheceram o direito à proteção de dados em sua Carta Maior, pelo menos não de maneira expressa. Conforme demonstrará exposição que se segue, o Brasil está no rol desses países.

[65] A Convenção foi novidade no contexto da regulação transnacional e deixou claro o teor constitucional da proteção de dados, senão vejamos: ”Article 1 – Object and purpose
The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").”. CONCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em 20 mar. 2021.

É pacífico o entendimento da doutrina brasileira de que o fenômeno da informação foi objeto de preocupação do legislador constituinte. Nesses termos, guardam relação direta com o tema diversas garantias constitucionais como a liberdade de expressão, o direito à resposta, o sigilo da fonte, a proteção à privacidade e vida íntima e o sigilo das comunicações[66], por exemplo.

Voltando-se para a proteção de dados no âmbito da vigilância estatal, recorte do trabalho, Jacqueline de Souza Abre e Dennys Antonialli destacam que, no artigo 5º da Constituição Federal de 1988, são três os principais incisos que tratam da limitação do Estado no ato de vigilância, organizados aqui no seguinte quadro:

Quadro 1 – Principais dispositivos constitucionais limitadores da vigilância estatal

Localização	Direito fundamental	Descrição do dispositivo	Dimensão protegida preponderante
Art. 5º, IV, CF	Liberdade de expressão	"é livre a manifestação do pensamento, sendo vedado o anonimato"	Positiva
Art. 5º, X, CF	Direito à privacidade	"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"	Negativa
Art. 5º, XII, CF	Sigilo das comunicações	"é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"	Negativa

Fonte: Sistematização própria, a partir do artigo "Vigilância sobre as comunicações no Brasil"[67]

Diante dos mencionados dispositivos, os autores constatam uma disputa interpretativa que se cinge principalmente ao inciso XII, tutela do sigilo das comunicações. Nesse contexto, dois pontos são relevantes: (i) se o objeto de proteção são as correspondências, comunicações telegráficas, dados e comunicações telefônicas em si ou apenas esses objetos enquanto fluxo/comunicação e; (ii) quais desses objetos de proteção estão incluídos na exceção mencionada ("salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal").

[66] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 185-216, jul./dez. 2018.
[67] ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.** São Paulo: InternetLab, 2017.

Quanto a esse segundo ponto, destaca-se que, em regra, a doutrina se consolidou no sentido de que apenas o sigilo das comunicações telefônicas podem ser objeto de exceção para fins de investigação criminal e instrução processual penal[68].

Dito isso, passa-se para análise mais acurada da primeira disputa hermenêutica, que tem maior relevância no contexto deste trabalho.

Focalizando o objeto referente aos "dados", é discutido se o sigilo conferido pelo dispositivo diz respeito aos dados *per si* ou apenas ao fluxo dos mesmos, ou seja, se somente dentro do fluxo de dados, "vigora um veto à entrada nessa comunicação"[69] para àqueles os quais os dados não foram endereçados. Nesse diapasão, o professor da Universidade de São Paulo, Tércio Ferraz Sampaio Junior, exerceu grande influência com o artigo "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado". Através da publicação, o jurista deu solidez ao entendimento de que o sigilo disposto no art. 5º, XII, da CF/1988, é limitado ao fluxo de dados. Tal conclusão é dada por linha argumentativa que se colaciona aqui em razão de sua relevância:

> O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas". Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. (...) Mas se alguém entra nesta transmissão, como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados.
>
> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação.70

---

[68] Apesar dessa consolidação, percebe-se nos tribunais uma tendência de abrir exceções para quaisquer das comunicações, a depender da situação. Nesse sentido: "Tal interpretação, mesmo que ainda respaldada por parte da doutrina, não reflete a jurisprudência dos tribunais, que passou a admitir "quebras" do sigilo do fluxo das comunicações de todos os tipos, isto é, não só de comunicações telefônicas, desde que "proporcionais", quando se fundamentarem em direito fundamental conflitante ou em interesse público" ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.** São Paulo: InternetLab, 2017. pp. 16-17.

[69] FERRAZ JR., Tercio Sampaio, Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado, in: **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 447, 1993.

[70] *Ibidem*. Grifos do autor. pp. 446- 447.

Em que pese esse entendimento, o jurista entendeu que os dados armazenados não estariam em um vazio protetivo na CF/1988, merecendo guarda em razão da tutela da privacidade (art. 5º, X, da CF/1988). Todavia, como verifica a doutrina[71], a lição do eminente Professor foi parcialmente absorvida pelo STF no sentido de que apenas o fluxo dos dados tem guarida constitucional, pelo menos em um primeiro momento. Tal entendimento teve relevante influência na Suprema Corte, cujas principais decisões nessa direção serão analisadas no próximo tópico.

Diante da consolidação dessa interpretação, a doutrina passa a constatar a insuficiência dos dispositivos constitucionais mencionados para uma tutela adequada dos titulares dos dados pessoais. Nessa direção, a Professora Laura Schertel Mendes elenca uma série de casos em que são patentes as limitações protetivas da privacidade e do sigilo das comunicações, como exemplo: (i) as informações raciais que alimentam algoritmos discriminatórios não podem ser consideradas íntimas ou pertencentes à vida privada, muito menos estão enquadradas no conceito de comunicação de dados; (ii) a mesma coisa para as informações referentes ao ajuizamento de ações trabalhistas, que alimentam as "listas negras" e; (iii) as informações relativas à participação em movimentos sociais ou reuniões em espaços públicos têm natureza eminentemente pública e não são coletadas a partir de comunicações privadas que garantiriam o sigilo[72].

Dessa forma, percebe-se, com clareza, que tais casos configuram graves ameaças a direito fundamentais e que, não obstante elevada magnitude na proteção de garantias individuais, os incisos constitucionais referentes à proteção da privacidade e do sigilo das comunicações não abarcam uma série de situações. Faz-se mister, portanto, um desenvolvimento constitucional de um direito autônomo à proteção de dados[73].

---

[71] QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tercio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n. 1, v. 1, p. 64-90, 2020.

[72] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, p. 194, jul./dez. 2018. Nesse sentido, Laura conclui que comum "a todos esses casos é o processamento ou a utilização de informações relacionadas a uma pessoa, que a identificam e a caracterizam. São, portanto, informações pessoais, sem se configurar, no entanto, em informações íntimas ou privadas. Tampouco se enquadram na garantia de sigilo da correspondência ou das comunicações, pois em nenhuma das hipóteses tratava-se de comunicação. E não obstante, percebe-se que essas informações merecem a proteção da ordem constitucional, na medida em que o seu processamento e a sua utilização acarretam a violação de outros direitos fundamentais." *Ibidem.* p. 194.

[73] A importância dessa construção constitucional do direito fundamental à proteção de dados pessoais fica clara nas palavras de Gustavo Gil Gasiola, Diego Machado e Laura Schertel Mendes: "Nota-se, portanto, o relevante papel que o direito fundamental à proteção de dados exerce no ordenamento: ele possibilita que todos os atos normativos que autorizem um determinado tratamento de dados tenham o seu conteúdo controlado para avaliar a

Nesse intento, encontram-se alternativas convergentes na doutrina. Esses esforços vislumbram formas de contornar essa exiguidade de um direito à proteção de dados expresso na Constituição Federal de 1988. Sobre a questão, o jurista constitucionalista Ingo Wolfgang Sarlet[74] entende que um implícito direito fundamental à proteção de dados pode e deve ser reconhecido a partir de um processo de recondução a diversas garantias fundamentais. Por exemplo, o professor visualiza referências ao direito em valores constitucionais de caráter geral como o princípio da dignidade da pessoa humana, o direito fundamental ao livre desenvolvimento da personalidade e ao próprio direito geral à liberdade, bem como em direitos específicos da personalidade, como a tutela da privacidade.

Todavia, Ingo compreende como base fundamental do direito à proteção de dados o direito ao livre desenvolvimento da personalidade, o qual, por sua vez, tem respaldo direto no princípio da dignidade humana e no direito geral de liberdade, culminando assim em "uma cláusula geral de proteção de todas as dimensões da personalidade humana"[75], manta protetiva sob a qual seguramente encontra-se a tutela de dados pessoais. Ante essa apreciação, o autor defende restar clara a consagração de um direito implícito à proteção de dados a partir de uma interpretação sistemática e harmônica da Constituição Federal de 1988.

Em complementariedade, a Professora Laura Schertel Mendes[76], da Universidade de Brasília, destaca a relevância do RE 673.707/MG para o deslinde da problemática. O precedente é significativo para a evolução da matéria no Supremo Tribunal Federal e, assim, será examinado com maior minúcia no próximo tópico. Todavia, cabe ressaltar por ora que o julgado concerne à aplicação do *habeas data*, garantia processual constitucional prevista no artigo 5º, LXXII, da Constituição Federal[77]. Já o caso concreto cingiu-se à possibilidade de contribuintes

---

adequação do referido tratamento. Isso ocorreu no famoso caso anteriormente analisado, assim como em outros julgados importantes na Alemanha, por exemplo, no caso de retenção de dados (BVerfGE Vorratsdatenspeicherung) e no caso de busca pela polícia de perfis suspeitos a partir do cruzamento de dados (BVerfGE Rasterfahndung)." GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A administração pública entre transparência e proteção de dados. **Revista do Direito do Consumidor.** São Paulo: RT. vol. 135/2021. p. 191. Maio-Jun/2021.

[74] SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, pp. 184-185, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.

[75] *Ibidem*. p. 185.

[76] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 195-198, jul./dez. 2018.

[77] " LXXII - conceder-se-á 'habeas-data':

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

terem acesso ao Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil – SINCOR.

Com resposta da Suprema Corte favorável aos contribuintes e seu entendimento por um escopo ampliado de dados que merecem proteção, vislumbra-se a existência implícita de um direito fundamental à proteção de dados pessoais. É que, como preleciona a jurista e o próprio Ministro Gilmar Mendes em seu voto, com a configuração de uma garantia processual de estatura constitucional como o *habeas data* tem-se o pressuposto lógico da existência de um direito material correspondente, voltado para a sustentação do remédio constitucional[78].

Noutro giro, é imprescindível também expor todo o esforço com desígnio em fixar a garantia à proteção de dados pessoais como direito fundamental expresso na Constituição Federal. Nesses termos, impende ressaltar a PEC nº 17/2019[79], que atualmente transita no Congresso Nacional. São dois os principais eixos de mudança proposta pela emenda: (i) inserir no artigo 5º, da CF, o inciso XII-A para a incluir a proteção de dados no rol de direitos fundamentais e; (ii) inserir no artigo 22, da CF, o inciso XXX para outorgar à União competência privativa para legislar sobre a matéria. A proposta já foi aprovada, de forma unânime, no Senado Federal, e encaminhada para Câmara dos Deputados.

Em geral, a doutrina vê com bons olhos a aprovação da emenda, em que pese já haja consolidado implicitamente um direito à proteção de dados. *Verbi gratia*, por um lado, Laura Schertel Mendes, Otávio Luiz Rodrigues Júnior e Gabriel Campos Soares da Fonseca[80] compreendem que o recente reconhecimento desse direito pela Suprema Corte brasileira confere urgência para a aprovação da PEC. No mesmo sentido, Ingo Wolfgang Sarlet enumera uma série de argumentos favoráveis à aprovação da emenda, que, segundo o autor, "agrega (ou,

---

[78] Nesse sentido, o Min. Gilmar Mendes afirmou: "Ao lado disso, temos essa situação específica que diz respeito a um direito subjetivo material, à proteção de dados ou à proteção dessa autonomia. Daí, a importância, me parece, deste julgado, que pode ser, talvez, o marco inicial de uma vitalização do habeas data, numa percepção mais ampla. (...) Em suma, há já uma reflexão, não no campo procedimental processual, mas também no campo do direito material." BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 673.707 Minas Gerais.** Rel. Min. Luiz Fux, Plenário, DJe 30/09/2015. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=307831711&ext=.pdf. Acesso em: 26 mar. 2021.

[79] BRASIL. **Proposta de Emenda à Constituição nº 17**, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em 27 mar. 2021.

[80] MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 61-71.

ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil."[81].

Nesse sentido, destacam-se os seguintes pontos colocados pelo Professor Ingo: (i) o direito à proteção dados expressamente positivado consolidaria uma posição autônoma independente da interação com outros direitos fundamentais e; (ii) garantiria uma inquestionabilidade quanto à plenitude de seu regime jurídico-constitucional, assegurando o gozo dessa posição em seu sentido formal e material. Sobre às vantagens conferidas por esse último ponto, o jurista ressalta (i) o *status* hierárquico elevado em razão da integração formal na Constituição, (ii) a aplicabilidade imediata (art. 5º, §1º, CF) e (iii) o atributo de limite material a reformas constitucionais[82].

Ante todo o exposto, não obstante a clara insuficiência dos direitos positivados expressamente na Constituição para regular integralmente o fenômeno da informação, fica evidente que a doutrina teve êxito em arquitetar acertadas linhas argumentativas a fim de identificar a existência de um implícito direito constitucional à proteção de dados pessoais, que preenche essa lacuna. Todavia, ainda é relevante a discussão para a consolidação dessa garantia de maneira expressa na Constituição Federal, que ganhou forma com a PEC nº 17/2019 e é essencial para conferir maior robustez jurídica constitucional à matéria.

2.2. CONSTRUÇÃO JURISPRUDENCIAL: do caminho ao reconhecimento do direito fundamental autônomo à proteção de dados até os questionamentos ao Decreto nº 10.046 na Suprema Corte brasileira

Nesta seção, como já mencionado, busca-se apresentar os principais precedentes sobre a matéria de proteção de dados no âmbito constitucional (STF) – posicionamentos que se modificaram no tempo e mostram-se, a partir de uma análise, em uma clara linha evolutiva. No intento de apresentar com clareza essa evolução, busca-se aqui exposição didática e cronológica dos julgados selecionados, bem como a apresentação de uma tabela resumo ao final do capítulo.

São as seguintes decisões escolhidas e suas respectivas relevâncias para o tema: (i) Mandado de Segurança nº 21.729/DF e Recurso Extraordinário nº 418.416/SC – a proteção à

[81] SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, pp. 184-185, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.
[82] *Ibidem.*

comunicação de dados (e não aos dados em si) prevista no art. 5º, XII, da CF; (ii) Recurso Extraordinário nº 673.707/MG – entendimento do conceito de dados em sentido amplo e gênese de um entendimento acerca de um direito fundamental material relacionado à proteção de dados; (iii) Ação Direta de Inconstitucionalidade nº 6.387/DF – estabelecimento do direito fundamento à proteção de dados como garantia constitucional autônoma e; (iv) Ação Direta de Inconstitucionalidade nº 6649/DF e Arguição de Descumprimento de Preceito Fundamental nº 695/DF – questionamentos constitucionais ao Decreto nº 10.046/2019, objeto de pesquisa.

Queiroz e Ponce[83] destacam que a tese constitucional sobre a proteção do sigilo dos dados (art. 5º, XII, CF) estar restrita à comunicação/fluxo desses, e não aos dados em si, teve as bases fundadas no MS nº 21.729/DF e no RE nº 418.416/SC. O *mandamus*[84], julgado na Suprema Corte brasileira em 1995, tratou de impetração do Banco do Brasil contra ato do Procurador-Geral da República, que requeria quebra de sigilo bancário através da entrega de dados de beneficiários de financiamentos públicos no setor rural, ato que o Banco do Brasil entendia ser condicionado à ordem judicial.

O parecer do – na época – Vice-Procurador-Geral da República foi inovador, carregando à Corte a argumentação de que o sigilo bancário não teria resguardo constitucional no caso. É que, segundo linha argumentativa, tratava-se de dados já recebidos e armazenados e, assim, conforme supracitado artigo do Tércio Sampaio Ferraz Júnior[85], não merecedores do sigilo disposto no art. 5º, XII, da CF, limitado aos dados em comunicação.

Não obstante o esforço aduzido, a principal *ratio* da decisão não se ateve a esses argumentos: a maioria fundamentou-se no princípio da publicidade às operações públicas, já que tratava de um financiamento concedido pelo Banco do Brasil. Todavia, dois Ministros vencedores (Sepúlveda Pertence e Francisco Rezek)[86] argumentaram expressamente em favor

---

[83] QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tercio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n. 1, v. 1, p. 71, 2020.

[84] BRASIL. **Mandado de Segurança nº 21.729 Distrito Federal.** Rel. Min. Marco Aurélio, Red. do Acórdão Min. Néri da Silveira, Plenário, DJ de 19/10/2001. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 Acesso em 15 abr. 2021.

[85] Vide nota 23. Nota-se, aqui, que o mesmo artigo científico poderia ser utilizado como argumento contrário à ausência de sigilo, porquanto, em que pese não considerar os dados armazenados protegidos pelo inciso XII, do art. 5º, ca CF, vislumbrou uma possível proteção desses dados pelo inciso X, do mesmo artigo.

[86] Exemplo disso é o seguinte trecho do voto do Min. Francisco Rezek: "Do inciso XII, por seu turno, é de ciência corrente que ele se refere ao terreno das comunicações: a correspondência comum, as mensagens telegráficas, a comunicação de dados, e a comunicação telefônica. Sobre o disparate que resultaria do entendimento de que, fora do domínio das comunicações, os dados em geral – e a seu reboque o cadastro bancário – são invioláveis, não há o que dizer. O funcionamento mesmo do Estado e do setor privado enfrentaria um bloqueio. A imprensa, destacadamente, perderia sua razão de existir." (grifos do autor) BRASIL. **Mandado de Segurança nº 21.729 Distrito Federal.** Rel. Min. Marco Aurélio, Red. do Acórdão Min. Néri da Silveira, Plenário, DJ de 19/10/2001.

do descabimento do sigilo das comunicações (art. 5º, XII, da CF) no tocante ao tema discutido, porquanto não se tratava de dados em comunicações, o que implicaria em uma desnecessidade de ordem judicial para que autoridades os acessassem. Esses entendimentos já configurariam um presságio da posição que o STF viria a tomar.

Nessa perspectiva, a decisão do RE nº 418.416/SC[87], tomada pelo Plenário da Suprema Corte brasileira em 2006, é paradigmática. No caso, o empresário proprietário das Lojas Havan, Luciano Hang, buscava reverter acórdão do TRF-4 que o condenava de crimes tributários. Os procuradores do advogado defendiam a ilicitude das provas que subsidiaram a resolução da causa: por mais que existisse ordem judicial para a busca e apreensão de equipamentos eletrônicos, não seria lícita a decodificação dos arquivos armazenados nas máquinas apreendidas.

Todavia, o Tribunal caminhou em sentido contrário. Liderado pelo Ministro Sepúlveda Pertence, relator da causa, o Plenário, por ampla maioria (dez votos a um), entendeu que não seria caso de inviolabilidade dos dados acessados. Nesse viés, o Ministro Relator – que já tinha adotado o entendimento da não guarida constitucional dos dados armazenados pelo sigilo do inciso XII, art. 5, da CF, no MS nº 21.729/DF – confirmou seu posicionamento, sendo que, dessa vez, sua *ratio decidendi* foi acompanhada pela maioria. Aliás, reforçando tal argumento, o Ministro Cezar Peluso aduziu que conferir tal sigilo aos dados armazenados conduziria a absurdos na medida em que influenciaria as pessoas a mover informações para meios tecnológicos com fins de fugir da atuação fiscalizadora estatal[88].

Estava, dessa forma, estabelecida no Supremo Tribunal Federal a tese de que dados pessoais em si não mereceriam a proteção proveniente do inciso XII, do art. 5º, da CF. Todavia, conforme já exposto, o desenvolvimento tecnológico não cessou, implicando em novos riscos e desafios à tutela constitucional da personalidade e, por conseguinte, dos dados pessoais.

Dessa forma, o STF teve em suas mãos a missão de se atualizar, seguindo um caminho inexorável que o levasse ao reconhecimento de um direito fundamental autônomo à proteção de dados. Nesse sentido, a decisão selecionada como de "meio do caminho" nesse processo foi

---

Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 Acesso em 15 abr. 2021.. pp. 119-120

[87] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416 Santa Catarina.** Rel. Min. Sepúlveda Pertence, Plenário, DJ de 19/12/2006. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em 15 abr. 2021.

[88] QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tercio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n. 1, v. 1, p. 73, 2020.

o RE nº 673.707/MG, que, julgada pelo Plenário do STF em 2015, teve êxito na compreensão dos dados pessoais em sentido amplo e iniciou o debate sobre um direito material fundamental relacionado à proteção de dados, senão vejamos.

O julgado diz respeito à demanda de um contribuinte que buscava ter conhecimento de informações que lhe diziam respeito, presentes no Sistema da Secreta da Receita Federal, mais especificamente, no Sistema de Conta Corrente da Secretaria da Receita Federal do Brasil (SINCOR). As razões do recorrente cingiam-se principalmente à proteção garantida pelo instituto do *habeas data* (art. 5º, LXXII, da CF), que deveria assegurar o conhecimento das "anotações, informações e dados (...), de forma que exista transparência da atividade administrativa, principalmente com relação a informações que digam respeito ao próprio contribuinte."[89].

A pretensão do contribuinte foi acolhida pelo Plenário do STF, e do aresto publicado pode-se depreender duas questões importantes para o desenvolvimento constitucional da tutela dos dados pessoais[90], são elas: (i) um entendimento inédito quanto à amplitude do conceito de dados, é dizer: o escopo de dados protegidos foi compreendido com extensão jamais reconhecida na Corte e; (ii) provocações iniciais quanto à existência de um direito material fundamental à proteção de dados pessoais ou, pelo menos, à autodeterminação informativa[91].

---

[89] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 673.707 Minas Gerais.** Rel. Min. Luiz Fux, Plenário, DJe de 30/09/2015. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=307831711&ext=.pdf. Acesso em 22 abr. 2021. p. 2 (relatório)

[90] Nesse sentido, vide: MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 195-199, jul./dez. 2018.

[91] Sobre esse ponto, destaca-se a diferenciação feita por Ingo entre os direitos à proteção de dados e autodeterminação informativa: "Na sua multicitada decisão, o Tribunal Constitucional Federal alemão, contudo, não reconheceu diretamente um direito fundamental à proteção de dados pessoais, mas, sim, deduziu (...) um direito fundamental implícito à autodeterminação informativa, que, consiste, em suma e de acordo com o Tribunal, na prerrogativa de cada indivíduo de decidir em princípio e substancialmente sobre a divulgação e utilização de seus dados pessoais. (...)
Ainda em sede preliminar, é de se observar que, nada obstante a circunstância de que o direito à proteção de dados pessoais guarda relação direta (mas, como já adiantado, não se confunde) com um direito à autodeterminação informativa – que, de todo modo, é um dos esteios e elementos centrais da proteção de dados – na sua condição de direito subjetivo, o catálogo de posições jusfundamentais que encerra é bastante diversificado." SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, pp. 189-195, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.

Sobre o primeiro ponto, destaca-se o posicionamento do Relator Ministro Luiz Fux que, conforme lições da doutrina atualizada sobre o tema[92], introduziu na Suprema Corte o entendimento de que os dados devem ser entendidos como "tudo que diga respeito ao interessado, seja de modo direto ou indireto."[93]. Nesse sentido, identifica-se que o escopo de proteção dos dados pessoais deve incidir em um âmbito mais amplo do que o preceituado pelo direito à privacidade, isto é, além de uma proteção reduzida à intimidade e vida privada, perfazendo uma salvaguarda a todos os dados associados ao cidadão.

Em segundo, destaca-se o entendimento do Ministro Gilmar Mendes sobre a necessidade de consolidação de um direito material à proteção de dados pessoais ou à autodeterminação informativa. Como pontua o Ministro, a garantia do instituto processual do *habeas data* carece de um direito fundamental material que o sustente e, à exemplo do direito alemão (decisão sobre o censo demográfico de 1983), poderia caber ao STF conceder contornos a essa garantia. Tal entendimento pode ser compreendido como uma inclinação inicial, ou mesmo um prenúncio, para a consolidação de um direito fundamental autônomo à proteção de dados pessoais no âmbito da Suprema Corte brasileira, como se depreende da recente decisão que se segue.

Por sua vez, a ADI nº 6.387/DF[94] é de importância ímpar para o desenvolvimento constitucional da matéria de proteção de dados, na medida em que reconheceu um direito fundamental autônomo à proteção de dados[95].

No caso concreto, o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB) pleiteou o reconhecimento da inconstitucionalidade da Medida Provisória nº 954/2020, que regulava o compartilhamento de dados pessoais (nomes, números de telefone e endereço) por empresas de telecomunicação com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de produção estatísticas por meio de entrevistas não presenciais, enquanto perdurava o estado de calamidade pública decorrente do coronavírus.

---

[92] Vide: CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lênio Luiz. **Comentários à Constituição do Brasil.** 1. ed. São Paulo: Saraiva, 2013. p. 487.

[93] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 673.707 Minas Gerais.** Rel. Min. Luiz Fux, Plenário, DJe de 30/09/2015. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=307831711&ext=.pdf. Acesso em 22 abr. 2021. p. 2 (ementa)

[94] Deveras, a decisão tratou das ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, propostas por, além do Conselho Federal da OAB, pelos partidos PSB, PSDB, PSol e PCdoB. Registre-se que optou-se por utilizar somente a numeração da ADI 6.387/DF para fins de simplificação.

[95] Nesse sentido: MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo.** In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 61-71.

Com efeito, os argumentos utilizados para sustentar a inconstitucionalidade foram atinentes a diversos pontos da MP nº 954/2020, dentre os quais se destacam: (i) a vagueza dos termos escolhidos na medida, como a finalidade de "produção estatística oficial", o que, junto às informações coletadas nas entrevistas, abriria espaços para a criação de perfis detalhados dos cidadãos a partir das modernas técnicas de coleta e processamento de dados; (ii) a desproporcionalidade dos dados compartilhados (os presentes nos sistemas das empresas de telecomunicação) com o necessário para desenvolver as pesquisas (dados amostrais); (iii) ausência de previsão de meios para o controle da segurança da informação a fim de evitar vazamentos ou usos indevidos, por exemplo, e; (iv) todo o cenário de insegurança é agravado em razão da ausência de uma autoridade nacional (como a ANPD, que à época ainda não se encontrava instituída) para a fiscalização do compartilhamento[96].

Diante da contenda, no ano de 2020, o Plenário do STF deferiu medida cautelar para suspender a eficácia da MP. Nessa direção, vislumbrou-se a existência de diversos riscos decorrentes do marco normativo e, por conseguinte, compreendeu não haver "interesse público legítimo no compartilhamento de dados pessoais dos usuários dos telefonia"[97].

Efetivamente, a Suprema Corte brasileira lançou mão de linha argumentativa da qual depreende-se claramente o reconhecimento de um direito fundamental autônomo à proteção de dados. Exemplo disso é (i) a menção a um conceito ampliado de dados pessoais para além da intimidade e vida privada – abarcando os dados "públicos", como nome, telefone e endereço – , perfazendo a ideia de inexistência de dados irrelevantes, bem como (ii) a recondução a outras garantias fundamentais como hermenêutica necessária para o reconhecimento do direito à proteção de dados, dessa forma, observa-se:

> Tais informações, relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o 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).[98]

---

[96] *Ibidem.* pp. 62-64

[97] BRASIL. **Ação Direta de Inconstitucionalidade nº 6.387 Distrito Federal.** Rel. Min. Rosa Weber, Plenário, DJe de 12/11/2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 24 abr. 2021. p. 2 (ementa)

[98] BRASIL. **Ação Direta de Inconstitucionalidade nº 6.387 Distrito Federal.** Rel. Min. Rosa Weber, Plenário, DJe de 12/11/2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 24 abr. 2021. p. 10 (voto da Min. Rosa Weber)

Ainda, ponto relevante citado no voto do Ministro Gilmar Mendes e que ainda será melhor examinado neste trabalho é o conceito de "devido processo informacional", que, em síntese, contém a ideia de que a tutela dos dados pessoais não é ferramenta para impedir o tratamento de dados, mas sim para criar parâmetros razoáveis a fim de compatibilizar os benefícios do tratamento e as garantias individuais e coletivas potencialmente em risco nesse processo.

Sobre o caráter histórico e a magnitude da relevância dessa decisão que reconheceu a autonomia do direito à proteção dos dados pessoais, destaca-se que o julgado passou a subsidiar a *ratio* de outras demandas no STF. Exemplo disso são os processos voltados ao reconhecimento de uma suposta inconstitucionalidade do Decreto nº 10.046/2019, ponto central do recorte de pesquisa desta monografia que se passa a analisar. Tal ato normativo editado pelo Executivo "dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados"[99].

Em primeiro, impende destacar a ADPF nº 695, proposta pelo Partido Socialista Brasileiro (PSB), onde impugnou-se ação lastreada no referido ato normativo do Poder Executivo. Trata-se de contestação às tratativas que visavam o compartilhamento dos dados de mais 76 milhões de brasileiros contidos nas bases do DENATRAN – como nomes, endereços, telefones, dados dos veículos e fotos do motorista habilitado com a Carteira Nacional de Motorista –, que seria executado pelo Serviço Federal de Processamento de Dados (SERPRO) em favor da Agência Brasileira de Inteligência (ABIN).

Ocorre que o Termo de Autorização nº 7/2020, do DENATRAN, que deferiu o compartilhamento de dados, foi revogado antes do julgamento da cautelar. O fato, todavia, não impediu de o Ministro Relator Gilmar Mendes debruçar-se sobre o processo, em razão da relevância de tema mais amplo, qual seja, "o plexo de medidas tendentes ao compartilhamento de dados pessoais pelos órgãos e entidades da Administração Pública com suposto lastro normativo no Decreto nº. 10.046."[100].

---

[99] BRASIL. **Decreto nº 10.046**, 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 mai. 2021.

[100] BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695 Distrito Federal.** Rel. Min. Gilmar Mendes, decisão monocrática, DJe de 29/06/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 05 mai. 2021. p. 46.

Dessa forma, ao considerar a manutenção do objeto da ação, o Ministro Gilmar Mendes prolatou, em sede de medida cautelar, decisão, cujos argumentos relevantes merecem destaque, tais quais: (i) a reafirmação do reconhecimento de um direito autônomo à proteção de dados; (ii) o entendimento de um "devido processo informacional" como corolário da garantia fundamental à proteção de dados; (iii) o entendimento da privacidade e da proteção de dados como valores fundamentais transindividuais; (iv) a compreensão dos princípios gerais da proteção de dados como decorrência direta desse direito fundamental e do princípio constitucional da legalidade; (v) a importância de um teste de proporcionalidade para aferir a constitucionalidade do compartilhamento de dados no Poder Público. Tais pontos consistem em importantes marcos teóricos que servirão de base para uma análise crítica e constitucional do Decreto nº 10.046/2019 no próximo capítulo. Demais disso, registre-se que, até a data de fechamento deste trabalho, não houve novas decisões nesta ADPF.

Noutro giro, na ADI nº 6.649/DF[101], defende-se a inconstitucionalidade do próprio Decreto nº 10.046/2019. Os questionamentos constitucionais recaem-se tanto em pontos materiais quanto formais, sendo que, alinhando-se ao objetivo desta monografia, cabe dar relevância para as supostas inconstitucionalidades materiais alegadas.

Nessa direção, o Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), impetrante da ação, desenvolve detalhada construção argumentativa, perfazendo o caminho da autonomia do direito à proteção de dados em relação ao direito à privacidade e contextualizando o desenvolvimento da proteção constitucional dos dados pessoais no Brasil. Ainda, cumpre ressaltar a percuciente exposição do impetrante sobre os princípios que decorrem diretamente da garantia fundamental à proteção de dados, quais sejam, os princípios da finalidade, da transparência, da adequação, da necessidade e da segurança da informação, todos já escrutinados neste trabalho.

Postas essas bases teóricas, o CFOAB passa a aduzir em favor da inconstitucionalidade do Decreto nº 10.046/2019, perpassando por vários pontos, desde a antiga problemática de um banco de dados centralizado, como ocorre no ato normativo a partir da previsão do Cadastro Base do Cidadão, até as polêmicas e descriteriosas condições para compartilhamento de dados entre os órgãos públicos.

Acrescente-se que, em consonância com as razões elencadas na inicial, a Associação Data Privacy Brasil de pesquisa, admitida como *amicus curiae*, também teceu relevantes

[101] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.649 Distrito Federal.** Rel. Min. Gilmar Mendes. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 03 mai. 2021.

argumentos, dentre os quais, sublinha-se o caso do *National Data Center*, o aspecto transindividual do direito à proteção de dados e a disposição de métricas objetivas para aferir a proporcionalidade de tratamentos de dados pessoais. Todas essas questões que serão abordadas de forma mais minuciosa no próximo capítulo.

Registre-se que, até o fechamento deste trabalho, não havia ocorrido a manifestação da Suprema Corte sobre a contenda, fato que não torna menos importante a exploração das petições, posta a relevância dos argumentos esposados – de grande relevância para o recorte de pesquisa selecionado.

Por derradeiro, com fins meramente de síntese didática, cumpre desenvolver o seguinte quadro acerca do desenvolvimento jurisprudencial exposto:

Quadro 2 – Desenvolvimento jurisprudencial: da proteção de dados ao Decreto nº 10.046/2019

Processo	Ano[102]	Pontos centrais
MS nº 21.729/DF	1995	Consolidação de que os dados protegidos pelo sigilo disposto no inc. XII, art. 5º, da CF/88, são apenas os que estão em fluxo; traduz-se em fase inicial da interpretação do STF, quando os dados pessoais em si não eram resguardados constitucionalmente.
RE nº 418.416/SC	2006	
RE nº 673.707/MG	2015	Inédito entendimento sobre o conceito dos dados pessoais em um espectro ampliado; consiste em fase intermediária, marcada por um "flerte" do STF com a existência de um direito autônomo à proteção de dados.
ADI nº 6.387/DF	2020	Fase final do processo histórico, que resultou no reconhecimento de um direito fundamental autônomo à proteção de dados.
ADPF nº 695/DF	2020	Impugnação a compartilhamento de dados pessoais no Poder Público respaldado no Decreto nº 10.046/2019; importante decisão cautelar do Ministro Gilmar Mendes, cujos argumentos destacam relevantes contornos do direito fundamental à proteção de dados.
ADI nº 6.649/DF	2020 – presente	Impugnação ao próprio Decreto nº 10.046/2019; riqueza argumentativa quanto à inconstitucionalidade do ato normativo; ausência de pronunciamento do Supremo sobre a demanda.

Fonte: Sistematização própria

[102] Aqui, é considerado o ano que ocorreu a decisão principal dentro do processo estudado. No caso da ADI nº 6.649/DF, sobre a qual não foi proferida decisão alguma sobre a questão de direito posta, considera o ano que se iniciou o processo até o presente.

CAPÍTULO III: O DECRETO Nº 10.046/2019 SOB UMA ÓTICA CONSTITUCIONAL

Limites constitucionais ao compartilhamento de dados pessoais na Administração Pública

Neste terceiro capítulo, busca-se desenvolver a parte central do trabalho. Isto é, após dispor acerca da existência e das bases teóricas de um direito constitucional autônomo à proteção de dados pessoais no direito alemão e brasileiro, examina-se, aqui, a pertinência dessa garantia fundamental com o Decreto nº 10.046/2019, que dispõe "sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados".

Para tanto, o capítulo foi dividido em três partes. A primeira delas pretende explorar as peculiaridades do tratamento de dados no setor público, ressaltando, entre outros pontos, a relevância da proteção de dados pessoais como valor de interesse público essencial para a garantia do próprio regime democrático. Em segundo, busca-se analisar o próprio Decreto nº 10.046/2019, explorando suas principais disposições. Finalmente, na terceira parte do capítulo, procura-se examinar o ato normativo a partir do direito fundamental à proteção de dados pessoais. Essa última parte é dividida em três eixos, relativos a: (i) considerações acerca da natureza dos dados pessoais para seu tratamento; (ii) salvaguardas e o devido processo informacional; e (iii) a proporcionalidade como condição legitimadora do tratamento de dados no setor público.

3.1. O TRATAMENTO DE DADOS PESSOAIS NO SETOR PÚBLICO: superação de uma visão individualista acerca da privacidade e proteção de dados

Não é discutível o fato de que o tratamento de dados pessoais configura-se como atividade inerente à ação do setor público, como já se verifica, há tempo, na escrituração de imóveis, registros de nascimentos e na atividade tributária, por exemplo[103]. Ocorre que a partir do acelerado desenvolvimento das tecnologias de informação e comunicação (TICs), a exploração das possibilidades tecnológicas para o tratamento de dados deve ser bem regulada a fim da mitigação dos riscos aos cidadãos. Esses, diferentemente de nas suas relações com

[103] Para compreensão do histórico de tratamento de dados pessoais no setor público, cf. páginas 271-275 de: WILMMER, Miriam. **O regime jurídico do tratamento de dados pessoais pelo Poder Público.** In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 271-288.

instituições privadas, estão expostos em face do Estado a uma relação de tratamento de dados contínuo, não se configurando como um processo voluntário ou episódico.

Sobre o tema, Miriam Wilmmer[104] ressalta que os dados pessoais têm papel essencial para consecução de diversas atividades estatais que visam garantir o bem-estar social e um Estado eficiente, tal qual a formulação de competentes políticas públicas, o que, todavia, não impede que os mesmos dados pessoais sejam utilizados para fins nefastos, como a intensa vigilância estatal e atividades discriminatórias. Não por outro motivo, Black e Stevens[105] compreendem que o tratamento de dados no setor público deve ir além da via do mero consentimento do titular dos dados, fundando-se sempre em sólidas justificativas quanto sua finalidade, necessidade e adequação.

Dessa forma, já impende adiantar questão que será examinada com maior profundidade em tópico posterior, qual seja: a tutela de proteção de dados, sobretudo no contexto de tratamento de dados no setor público, não deve implicar em uma liberdade negativa do cidadão em face do estado, mas sim no oferecimento de salvaguardas adequadas para que o tratamento de dados pessoais proceda de forma a não violar direito fundamentais. É dizer: deve-se focalizar em um "devido processo informacional", que garanta mecanismos adequados para uma utilização eficiente de dados pessoais pelo Estado sem com que isso incorra em graves riscos para os cidadãos, ou seja, um tratamento de dados que sempre priorize a harmonização do interesse público e dos direitos individuais.

Nessa direção de estabelecimento de um processamento de dados pessoais no setor público de forma eficiente e segura, deve-se impreterivelmente apartar recorrente incorreção: a falsa tensão entre a privacidade e proteção de dados, de um lado, e o interesse público, de outro. O problema daí decorrente é a arquitetura de argumentos no sentido de que os princípios da eficiência e da supremacia do interesse público funcionam como justificativa universal para legitimar qualquer tratamento de dados pessoais no setor público, já que a privacidade e a proteção de dados seriam interesses particulares e, assim, deveriam curvar-se àqueles.

---

[104] WILMMER, Miriam. **O regime jurídico do tratamento de dados pessoais pelo Poder Público.** In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021, pp. 272-274.

[105] BLACK, Gillian e STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector**: The Critical Role Of Proportionality And The Public Interest. Scripted. Vol. 10, n. 1, 2013. Disponível em: https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest/ acesso em: 19 jul. 2021.

Ao revés, deve-se extirpar essa ideia de prevalência abstrata do interesse público em face da privacidade e proteção de dados, porquanto, como já repisado neste trabalho, há muito que não se fala em uma dimensão exclusivamente individualista da proteção de dados[106]. De qualquer forma, como bem pontua Daniel Sarmento[107], não é devido o afastamento automático e abstrato de direitos fundamentais em detrimento da supremacia do interesse público, necessitando, caso a caso, desenvolver adequada ponderação entre os valores em jogo.

Em recorte mais específico, há relevante riqueza bibliográfica que cuida com afinco da íntima relação existente entre proteção de dados pessoais, direito à privacidade e democracia, conferindo claros contornos de relevância pública e coletiva às garantias fundamentais ligadas à tutela dos dados pessoais e à privacidade. Na seminal obra *Privacy and Freedom*[108], escrita em 1968, o célebre Alan Westin já alertava para uma série de riscos que violações à privacidade poderiam culminar na sociedade e seus reflexos diretos no regime democrático, como exemplo, o enfraquecimento da liberdade de associação, o desincentivo à produção científica e a ação policial inadequada.

Dessa forma, relevantes lições doutrinárias compreendem a privacidade e, consequentemente, a proteção de dados pessoais, como valores essenciais para que os cidadãos criem um vínculo de confiança com a Administração Pública, condição obrigatória para que as pessoas possam expressar de forma livre seus julgamentos e opiniões. Só assim, segundo Ruth Gavison, é possível vislumbrar a "autonomia moral do cidadão"[109].

Em consonância, Daniel Solove[110] ressalta o "valor social" da privacidade. Para o autor, essa interpretação de relevância transindividual em nome da privacidade faz sentido na medida

---

[106] Nesse sentido, colaciona-se lição de Marcel Leonardi: "Isso significa que não se deve entender a tutela da privacidade como a proteção exclusiva de um indivíduo, mas sim como uma proteção necessária para a manutenção da estrutura social. A privacidade não é valiosa apenas para a vida privada de cada indivíduo, mas também para a vida pública e comunitária" LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2012. p. 122.

[107] SARMENTO. Daniel. **Supremacia do interesse público?** As colisões entre direitos fundamentais e interesses da coletividade. In: ARAGÃO, Alexandre Santos de; MARQUES NETO, Floriano Azevedo. **Direito administrativo e seus novos paradigmas.** Belo Horizonte: Fórum, 2008. p. 97-143.

[108] WESTIN, Alan Furman. **Democracy and Freedom**. New York: IG Publishing. 1968. p. 45-46. (ebook)

[109] RUTH, Gavison. Privacy and the Limits of the Law. **The Yale Law Journal**. vol. 89, no 3, p. 455, jan/1980. Em sentido similar, Colin Bennett e Smith Oduro-Marfo: "a política de proteção da privacidade serve mais para fortalecer a confiança, para dar aos cidadãos a garantia de que eles podem se envolver com suas instituições democráticas sem medo de serem monitorados e perseguidos injustamente." (Tradução livre: "privacy protection policy serves more to bolster trust, to give citizens the guarantee that they can engage with their democratic institutions without fear that they will be unfairly monitored and persecuted.") BENNET Colin; ODURO-MARFO, Smith. **Privacy, Voter Surveillance, and Democratic Engagement:** Challenges for Data Protection Authorities. International Conference of Data Protection and Privacy Commissioners (ICDPPC), Greater Victoria, 2019.

[110] SOLOVE, Daniel. **Understanding Privacy.** Cambridge: Harvard University Press, 2008.

em que essa garantia implica em extenso efeito sobre as estruturas de poder e liberdades da sociedade, configurando-se, por exemplo, como requisito indispensável para as discussões acerca de mudanças políticas e de elaboração de contracultura de forma livre e afastada de uma vigilância punitiva[111].

Portanto, quando proposto o processamento de dados pessoais no âmbito público, não se deve afastar os cuidados existentes no setor privado contra as possíveis violações. Não há que falar de forma alguma em uma prerrogativa abstrata e livre para o tratamento de dados em nome da eficiência pública e supremacia do interesse público. Ao contrário, deve-se ponderar caso a caso a legitimidade do tratamento através da lente do princípio da proporcionalidade, e sempre com vistas aos corolários do próprio direito fundamental à proteção de dados, como os princípios da finalidade, adequação, necessidade e segurança da informação.

Por fim, conferindo maior força argumentativa ao rol dos fundamentos dispostos neste tópico, vale ressaltar a reflexão de Clarisa Long, professora da Columbia Law School. Considerando o cenário pandêmico do Covid-19 e as diversas medidas emergenciais utilizadas pelos Estados, a estudiosa alerta para o aprendizado histórico de que, vez estabelecido poderes governamentais de vigilância, é muito improvável que os cidadãos possam fazer algo para mitigar a força estatal nesse âmbito. Mais do que isso, a professora adverte também que, depois de coletados, é difícil evitar que os dados não sejam utilizados para outros fins[112]. Frisa-se que essa situação vai além do momento pandêmico, isto é, medidas de vigilância adotadas, de qualquer forma e em qualquer tempo, sofrem fortes resistências para serem desfeitas.

Em face do exposto, é essencial a compreensão da privacidade e proteção de dados pessoais como valores transindividuais em razão das sérias repercussões que exercem na vida da sociedade e na própria estrutura governamental democrática. É sob essa lente que será analisado o Decreto nº 10.046/2019, aliada evidentemente a toda a construção teórica e dogmática acerca do direito fundamental à proteção de dados pessoais desenvolvida nos

---

[111] Sobre o assunto, conferir também: REGAN, Priscilla. **Legislating Privacy**: Technology, Social Values and Public Policy. Chapel Hill: University of North Carolina Press; FRAZÃO, Ana. **Proteção de dados e democracia:** a ameaça da manipulação informacional e digital. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antônio. **A Lei Geral de Proteção de Dados Pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paula: Revista dos Tribunais. 2021.

[112] " History teaches us that once established, governmental powers of surveillance of, and data collection on, its citizens and residents is unlikely to be voluntarily scaled back.14 And history has also taught us that once data is collected for one purpose it is difficult to prevent it from being used for other unrelated purposes." LONG, Clarisa. **Privacy and Pandemics**. In: PISTOR, Katharina. **Law in the time of COVID-19**. Columbia Law School Books, 2020. p. 92.

capítulos anteriores. Assim, passa-se a estudar as disposições do ato normativo selecionado como recorte de pesquisa.

3.2. O DECRETO Nº 10.046/2019:

O Decreto nº 10.046/2019 faz parte de um processo que visa a interoperabilidade de dados na Administração Pública. Tal movimento tem respaldo argumentativo principalmente nos objetivos de desburocratização do serviço administrativo e de melhoria da eficiência da prestação de serviços públicos e das execuções das políticas públicas[113].

Antes de adentrar no ato normativo em si, firma-se que a natureza de tal medida é digna e meritória, contudo, deve-se atentar para os meios pelo qual é desenvolvida, relembrando que o direito à proteção de dados pessoais é um direito de meio e não de fim. É dizer: a proteção de dados pessoais é garantia que visa não vedar e impossibilitar o tratamento, mas sim protegê-lo com as devidas salvaguardas.

Dada tal premissa, é vez de analisar o próprio Decreto nº 10.046/2019[114], que dispõe "sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados". Tal tarefa será desenvolvida mediante a apresentação de quatro eixos: (i) finalidades e conceitos; (ii) níveis de compartilhamento de dados; (iii) Cadastro Base do Cidadão; e (iv) Comitê Central de Governança de Dados.

Sobre o primeiro ponto, o artigo 1º estabelece as cinco finalidades[115] que guiam o ato normativo, todas elas voltadas para o aumento da eficiência do poder público em suas atividades

---

[113] Cf. "O contexto do Cadastro Base do Cidadão"

[114] BRASIL. **Decreto nº 10.046**, 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 mai. 2021.

[115] Art. 1º Este Decreto estabelece as normas e as diretrizes para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União, com a finalidade de:

I - simplificar a oferta de serviços públicos;

II - orientar e otimizar a formulação, a implementação, a avaliação e o monitoramento de políticas públicas;

III - possibilitar a análise das condições de acesso e manutenção de benefícios sociais e fiscais;

IV - promover a melhoria da qualidade e da fidedignidade dos dados custodiados pela administração pública federal; e

que envolvem o tratamento de dados (inclusive os pessoais), como a simplificação da oferta de serviços públicos e a melhoria da qualidade e fidedignidade dos dados em suas mãos. O que resta claro neste dispositivo inicial são as ausências da proteção de dados e segurança da informação como objetivos do diploma, em que pese o paradigma atual que confere ampla relevância a esses temas e os recentes problemas de vazamento de dados na Administração Pública, como ocorreu no Superior Tribunal de Justiça[116].

Quanto aos conceitos dispostos no artigo 2º do ato normativo, resta patente a incongruência da seleção léxica feita no diploma jurídico em relação às principais legislações nacionais que cuidam do tema de tecnologia e dados pessoais, sobretudo a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

Nesse contexto, destaca-se a categorização dos dados pessoais em atributos biográficos (art. 2º, I) – dados relativos a fatos da vida das pessoas, abarcando desde nome e data de nascimento até endereço e vínculos empregatícios – e atributos biométricos (art. 2º, II) – dados relativos a características biológicas ou comportamentais do indivíduo, como digitais dos dedos, formato da face e maneira de andar. Percebe-se, dessa forma, distanciamento da diferenciação da LGPD em "dados pessoais" e "dados pessoais sensíveis", não desenvolvendo, aliás, qualquer menção a estes últimos, que são objeto de atenção e regime especial na LGPD.

Ainda, há a previsão da constituição de bases integradoras (art. 2º, VI), bases de dados compostas por bases temáticas (art. 2º, VII), que, por sua vez, são integradas por dados biométricos ou biográficos para determinada política pública[117]. O que já pode ser considerado problemático pelo acúmulo de dados pessoais em um único espaço.

Por último no que diz respeito ao primeiro ponto, outra questão que chama atenção é o distanciamento conceitual entre as figuras do "gestor de dados" (art. 2º, XIII, do Decreto nº 10.046/2019), de um lado, e do "controlador" e "operador", da LDPG, por outro lado. O que se

---

V - aumentar a qualidade e a eficiência das operações internas da administração pública federal.

[116] Cf. https://oglobo.globo.com/brasil/ataque-hackerbloqueou-base-de-dados-do-stj-paralisou-totalmente-os-trabalhos-no-tribunal-1-24730440

[117] Art. 2º Para fins deste Decreto, considera-se:

(...)

VI - base integradora - base de dados que integra os atributos biográficos ou biométricos das bases temáticas;

VII - base temática - base de dados de determinada política pública que contenha dados biográficos ou biométricos que possam compor a base integradora;

depreende da leitura do Decreto é que, diversamente do positivado na legislação de proteção de dados, não há clareza quanto à obrigação imputada ao "gestor de dados" em termos de prestação de contas e responsabilização.

Sobre o segundo ponto, o capítulo II inicia parte central do ato normativo analisado: a nivelação dos dados pessoais para fins de compartilhamento. *In verbis* (grifo do autor):

> Art. 4º O compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º é categorizado em três níveis, de acordo com sua confidencialidade:
> I - **compartilhamento amplo**, quando se tratar de dados públicos que não estão sujeitos a nenhuma restrição de acesso, cuja divulgação deve ser pública e garantida a qualquer interessado, na forma da legislação;
> II - **compartilhamento restrito**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a todos os órgãos e entidades de que trata o art. 1º para a execução de políticas públicas, cujo mecanismo de compartilhamento e regras sejam simplificados e estabelecidos pelo Comitê Central de Governança de Dados; e
> III - **compartilhamento específico**, quando se tratar de dados protegidos por sigilo, nos termos da legislação, com concessão de acesso a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei, cujo compartilhamento e regras sejam definidos pelo gestor de dados.[118]

Nos próximos artigos, passa-se a regular especificamente cada um dos níveis de compartilhamentos. Em primeiro, nas disposições gerais, merece destaque a dispensa do requisito de "celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos e as entidades", observando-se "o disposto na Lei nº 13.709, de 2018 [LGPD]" (art. 5º).

Adentrando nos níveis específicos, sobre o compartilhamento amplo de dados, dispõe o Decreto que, no caso, é dispensada autorização prévia e deve ser feito mediante canais abertos específicos para os dados deste nível (art. 11). Em relação ao compartilhamento restrito, o ato normativo estabelece que a formulação de regras para a partilha de dados fica a cargo do Comitê Central de Governança de Dados (art. 12), abrindo a possibilidade para retransmissão desses dados pelo órgão ou entidade que o recebera (art. 12, § 4º). Quanto ao compartilhamento específico de dados, o diploma jurídico prevê, em síntese, que este deve ser condicionado à permissão do gestor de dados e dos requisitos dispostos pelo mesmo (art. 14, I e II), bem como, via de regra, proíbe a retransmissão de dados (art. 14, § 2º).

---

[118] BRASIL. **Decreto nº 10.046**, 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 mai. 2021.

Sintetizando o exposto, impende colacionar o seguinte quadro desenvolvido pelo Comitê Central de Governança de Dados:

Quadro 3 – Níveis de Compartilhamento previstos no Decreto nº 10.046/2019

Categoria	Descrição	Regras de compartilhamento
Ampla	Dados não protegidos por norma, portanto públicos.	Dispensa autorização prévia pelo gestor de dados e será realizada pelos canais existentes para dados abertos e transparência ativa. (art. 11)
Restrita	Dados protegidos por norma e compartilhados dentro do governo sem necessitar permissão.	Regras estabelecidas pelo Comitê Central de Governança de Dados. (art. 12)
Específica	Dados protegidos por norma, cujo compartilhamento depende de decisão do gestor de dados.	Condicionado à permissão de acesso pelo gestor de dados e ao atendimento dos requisitos definidos por este como condição para o compartilhamento. (art. 14) Os dados recebidos por compartilhamento específico não serão retransmitidos ou compartilhados com outros órgãos ou entidades, exceto quando previsto expressamente na autorização concedida pelo gestor de dados ou se houver posterior permissão desse (art. 12, §2º).

Fonte: Comitê Central de Governança de Dados[119]

Noutro giro, adentra-se no terceiro ponto, qual seja, a instituição do Cadastro Base do Cidadão – CBC, regulado no Capítulo IV do Decreto nº 10.046/2019. O CBC é, na realidade, uma grande base de dados centralizada: base integradora composta por uma série de bancos de dados (bases temáticas) associados ao Governo Federal (art. 17). As suas finalidades (art. 16), em harmonia com próprio ato normativo, fazem referência somente à eficiência pública (*v.g.*, "aprimorar a gestão de políticas públicas", "viabilizar a criação de meio unificado de identificação do cidadão para a prestação de serviços públicos" e "facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública"), ignorando qualquer menção à privacidade e proteção de dados.

Portanto, buscou-se criar no Cadastro Base do Cidadão uma ferramenta de disponibilização de dados de modo que favoreça à interoperabilidade desses elementos no setor público. Para tanto, busca-se a máxima acumulação possível de dados. Nesse sentido, cumpre ressaltar a composição inicial do CBC, formado a partir da base temática do CPF (art. 19), contando com um conjunto de dados biográficos (por exemplo, nome, sexo, filiação, naturalidade, etc.), desenvolvendo-se, ao passar do tempo, com o acréscimo de novos atributos

[119] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras para Compartilhamento de Dados.** 4 mai. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf. Acesso em 31 jul. 2021. p. 7.

biográficos, biométricos e cadastrais, sempre associados ao número de inscrição de CPF (art. 19, § 2º).

A principal crítica à criação do CBC remete a discussões das décadas 60 e 70. No período, a ascensão do paradigma do Estado Social aliada à revolução informática e da capacidade de processamento de dados expôs ideias ao redor do globo de formular sistemas informáticos centralizados para o tratamento de dados pessoais. Contudo, observou-se que, ao mesmo tempo que, de um lado, poder-se-ia ganhar com a eficiência administrativa, colocar-se-ia, de outro, em risco à privacidade e outras garantias fundamentais, em razão dos riscos de vazamento em uma base unificada e do próprio uso inadequado do Estado em nome de uma vigilância invasiva e abusiva. Tendo em vista o debate posto, em casos paradigmáticos como nos Estados Unidos (*National Data Center*) e na França (*SAFARI*), mostraram-se preferência por não assumir o risco e barrar as propostas das bases de dados unificadas.

O quarto e último ponto de destaque sobre o Decreto diz respeito a seu Capítulo V, que cuida da instituição do Comitê Central de Governança de Dados (CCGD), a quem é outorgado, entre outras responsabilidades (art. 21, I a XIII), deliberar: sobre as diretrizes para a categorização de compartilhamento, sobre a segurança da informação no compartilhamento de dados, sobre a inclusão de dados no CBC, etc. Como se observa claramente, na mesma linha que segue todo decreto, esta disposição não delimita com precisão os critérios e as regras adotadas, o que deixa um amplo espaço discricionário para que o Comitê decida sobre as questões.

Essa matéria mostra-se ainda mais preocupante em razão do desenho institucional selecionado no ato normativo. O artigo 22 ocupa-se de dispor sobre a composição[120] do Comitê, integrando-o apenas com funcionários da administração direta federal. Poder-se-ia argumentar que tal ausência de uma organização multissetorial seria suprida com a previsão dos subcomitês

[120] Art. 22. O Comitê Central de Governança de Dados é composto por representantes dos seguintes órgãos e entidade:

I - dois do Ministério da Economia, dentre os quais um da Secretaria Especial de Desburocratização, Gestão e Governo Digital, que o presidirá, e um da Secretaria Especial da Receita Federal do Brasil;

II - um da Casa Civil da Presidência da República;

III - um da Secretaria de Transparência e Prevenção da Corrupção da Controladoria-Geral da União;

IV - um da Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República;

V - um da Advocacia-Geral da União; e

VI - um do Instituto Nacional do Seguro Social.

técnicos (art. 21, X e § 3º), o que, na verdade, é insuficiente, na medida em que os subcomitês detêm apenas força de assessoramento, e não poder deliberativo. Dessa forma, observa-se vulnerabilidade na composição e nas competências do CCGD, que podem implicar em choque de interesses que vão de encontro ao bem público.

Por fim, outra crítica direcionada à criação do CCGD[121] diz respeito à compatibilização do órgão com a Autoridade Nacional de Proteção de Dados (ANPD), prevista na LGPD. No caso, chama a atenção que o Decreto estudado não tenha feito qualquer referência à ANPD, em que pese o posicionamento central dessa Autoridade como fiscalizadora e reguladora da proteção de dados no país e, mais especificamente, seu papel para fins de aplicações de sanções e uniformização interpretativa no que é relativo ao tema[122]. Ao revés, o Decreto nº 10.046/2019 outorga ao CCGD a competência para a resolução de controvérsias no compartilhamento de dados entre os órgãos públicos abarcados pelo diploma jurídico.

Portanto, facilmente depreende-se que o silêncio do ato normativo em relação à ANPD, e até mesmo a disposição de normas que entram em conflito com as competências desta Autoridade, implica em um grande problema, traduzido na superposição dos órgãos e nos riscos à proteção de dados pessoais.

3.3. O ATO NORMATIVO E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS:

3.3.1. NATUREZA DOS DADOS PESSOAIS: a superação de uma análise ontológica dos dados pessoais para sua tutela

[121] Cf. Petição inicial da ADI 6695. BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.649 Distrito Federal**. Rel. Min. Gilmar Mendes. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 03 mai. 2021.

[122] Art. 55-K. A aplicação das sanções previstas nesta Lei compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública.

Parágrafo único. A ANPD articulará sua atuação com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

Conforme o exposto no Capítulo I deste trabalho, um dos grandes êxitos da decisão alemã sobre o censo demográfico de 1983 foi reconhecer a inexistência de dados pessoais isentos de tutela em razão de sua natureza. Na oportunidade, a Suprema Corte alemã anteviu no crescente desenvolvimento tecnológico e nas novas possibilidades oriundas do processamento de dados um grave risco à dignidade da pessoa humana e à tutela da personalidade. Dessa forma, reconheceu como corolário da autodeterminação informativa a inexistência de dados insignificantes, vez que, com a utilização das mencionadas tecnologias e do processamento automático de dados pessoais, poder-se-ia transmutar dados aparentemente irrelevantes em informações detalhadas e valiosas sobre a intimidade, privacidade e/ou personalidade dos cidadãos.

Não por outro motivo Laura Schertel Mendes afirma que "o risco do processamento de dados residiria mais na finalidade do processamento e nas possibilidades de processamento do que no tipo dos dados mesmos"[123]. É dizer: a legitimidade do processamento de dados pessoais depende muito menos de uma análise sobre seus aspectos ontológicos – referentes à natureza – , e muito mais sobre os aspectos relacionados ao contexto de tratamento[124].

Voltando-se com grande profundidade aos aspectos da privacidade e ciência da informação, a Professora Helen Nissenbaum desenvolveu a célebre teoria da "integridade contextual"[125] como marco de referência essencial para a proteção da privacidade. A principal crítica feita é acerca dos termos gerais em que são estruturados os parâmetros de verificação de violação à privacidade, desprezando uma série de fatores contextuais imprescindíveis para o julgamento da questão.

Para a autora, a natureza dos dados pessoais configura como apenas um dos pontos relevantes para a ponderação acerca da legitimidade da coleta e processamento dos dados pessoais, devendo estar ao lado de, por exemplo, a natureza e contexto da situação de tratamento, a função dos agentes que recebem a informação, os termos de compartilhamento da informação pelo sujeito e da divulgação posterior[126].

---

[123] MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 11, out./dez. 2020.

[124] Daí percebe-se a natureza processual do direito fundamental à proteção de dados: é o contexto (processo) em que os dados pessoais são tratados que vão dizer a legitimidade (ou não) do respectivo tratamento. Essa ideia é a base do próximo tópico, onde a questão será aprofundada e debatida em face do Decreto nº 10.046/2019.

[125] NISSENBAUM, Helen. Privacy as Contextual Integrity. **Washington Law Review**, v. 79, pp. 101-139. 2004. Disponível em: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf. Acesso em 31 jul. 2021.

[126] Nesses termos: "(...) develops a model of informational privacy in terms of contextual integrity, defined as compatibility with presiding norms of information appropriateness and distribution. Specifically, whether a particular action is determined a violation of privacy is a function of several variables, including the nature of the situation, or context; the nature of the information in relation to that context; the roles of agents receiving information; their relationships to information subjects; on what terms the information is shared by the subject;

Adentrando a lógica do Decreto nº 10.046/2019, percebe-se que se optou por método distinto, de modo a distribuir as regras gerais de procedimento em três grandes "caixas" – compartilhamento amplo, restrito e específico. Por exemplo, sobre o compartilhamento amplo, rememora-se que se "dispensa autorização prévia pelo gestor de dados e será realizado pelos canais existentes para dados abertos e para transparência ativa" (art. 10). Além disso, regulação do Comitê Central de Governança de Dados determina que se incluem nesse nível amplo todos dados "não protegidos por norma, portanto públicos"[127].

Dessa forma, resta patente a primeira incongruência do ato normativo com o direito fundamental à proteção de dados: o corolário de que não existe dados insignificante é violado. Claramente, a facilidade oriunda de colocar todos os dados públicos em um canal aberto ignora o poder do processamento automático a partir do cruzamento de dados. Ainda, observa-se que tal fato não considera as peculiaridades de cada contexto específico, ignorando as diferenciações dos dados públicos e das circunstâncias de tratamento.

Nesse sentido, exemplo de um possível problema consiste na disponibilização de informações relativas a beneficiários de programas sociais. Em face da vulnerabilidade desse público, esses dados podem ser utilizados, por exemplo, para direcionamento e manipulação de questões políticas (*microtargeting*) e para prática de fraudes[128].

Dada essa problemática do diploma jurídico de supervalorização da natureza dos dados pessoais para definição dos caminhos normativos para compartilhamento desses dados, passa-se, agora, a análise essencial para aferir a constitucionalidade do Decreto nº 10.046/2019, qual seja, o cumprimento ou não dos ensinamentos provenientes da ideia de um devido processo informacional.

---

and the terms of further dissemination". NISSENBAUM, Helen. Privacy as Contextual Integrity. **Washington Law Review**, v. 79, p. 136-137. 2004. Disponível em: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf Acesso em 31 jul. 2021.

[127] COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras para Compartilhamento de Dados.** 4 mai. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf. Acesso em 31 jul. 2021. p. 7.

[128] Cf. Petição do *amicus curiae* do Laboratório de Políticas Públicas e Internet – LAPIN (e-Doc. 44, p. 22) em: BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.649 Distrito Federal**. Rel. Min. Gilmar Mendes. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 03 mai. 2021.

3.3.2. DEVIDO PROCESSO INFORMACIONAL: leitura da tutela dos dados pessoais como proteção eminentemente processual

Por um lado, é indiscutível que o crescente desenvolvimento tecnológico – instituidor da atual "era digital" – gera a legítima expectativa nos cidadãos de terem a interação com o Estado e o acesso aos serviços públicos facilitados. O atendimento dessas expectativas implica no almejado e legítimo *"Data-Driven Public Sector"*[129], modelo da administração pública dotada do auxílio da tecnologia e do processamento automático de dados e voltada exatamente para a maior eficiência do Estado na prestação de seus serviços e na comunicação com seus governados.

Por outro lado, como buscou-se apresentar no caminhar deste trabalho, o mesmo desenvolvimento da tecnologia e de suas ferramentas de processamento de dados culminou no alargamento dos riscos de violações à privacidade e a diversos outros direitos fundamentais dos cidadãos. Assim, tal conjuntura fez necessária a atualização do saber jurídico para a formulação do direito fundamental à proteção de dados.

Essa garantia fundamental, portanto, visa exatamente compatibilizar esses dois valores essenciais, de forma que viabilize o tratamento de dados pessoais pela Administração Pública em nome da eficiência ao mesmo tempo que são resguardados os direitos fundamentais dos cidadãos postos em risco nessa atividade. É exatamente por isso que se fala de uma natureza eminentemente processual, isto é, diversamente do caráter predominantemente negativo do direito à privacidade, o direito fundamental à proteção de dados pessoais não pretende impedir o processamento dos dados, mas sim que esse ocorra com a garantia das salvaguardas adequadas[130].

Nesse sentido, Bruno Bioni destaca sobre "a percepção de que o titular dos dados pessoais amarga uma (hiper)vulnerabilidade, o que demanda, respectivamente, o seu empoderamento para emancipá-lo e a sua intervenção para assisti-lo."[131]. Isso deve se dar exatamente com o devido processo informacional, maneira de municiar os titulares de dados e

---

[129] Cf. Organisation for Economic Co-operation and Development – OCDE. **The Path to Becoming a Data-Driven Public Sector**. OECD Publishing: Paris, 2019.

[130] Sobre o tema, afirma o Professor Danilo Doneda: "a resposta se aproxima da constatação de que a proteção de dados pessoais seria uma garantia de caráter instrumental, derivada da tutela da privacidade, mas que não poderia estar limitada por esta, ao mesmo tempo em que faz referência a todo leque de garantias fundamentais que se encontram no ordenamento brasileiro"

[131] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020. Introdução e Visão Geral (e-book).

a sociedade como um todo com as ferramentas necessárias para os fins de dirimir a grande assimetria informacional existente na relação cidadão-Estado[132].

Aliás, em sede dos precedentes da Suprema Corte brasileira, o Ministro Gilmar Mendes já reconheceu a centralidade do devido processo informacional como contorno da dimensão subjetiva do direito fundamental à proteção de dados, senão vejamos:

> É possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro "devido processo informacional" (informational due process privacy right), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.[133]

Aprofundando-se nos detalhes do devido processo informacional e colocando-o frente ao Decreto nº 10.046/2019, o primeiro ponto que merece destaque diz respeito aos princípios decorrentes do direito fundamental à proteção de dados, ponto imprescindível para a verificação de um devido processo[134]. Sobre o ponto, pode-se dizer que o ato normativo padece por sérias deficiências, como se passa a observar.

Em primeiro, ressalta-se o valor central dado ao princípio da finalidade desde a decisão alemã sobre o censo demográfico de 1983[135], donde infere-se a obrigação de todo tratamento

---

[132] "É exatamente para evitar o crescimento da assimetria informacional e colocar em xeque relações de poder que o devido processo informacional se mostra como uma garantia cada vez mais necessária. Aliás, a própria autonomia do direito à proteção de dados pessoais frente ao direito à privacidade está enraizada nessa racionalidade de devido processo" BIONI, Bruno; MARTINS, Pedro. **Devido processo informacional:** um salto teórico-dogmático necessário? JOTA, 15 jul. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020. Acesso em 05 ago. 2021.

[133] BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695 Distrito Federal**. Rel. Min. Gilmar Mendes, decisão monocrática, DJe de 29/06/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 05 mai. 2021.

[134] Rememora-se que, no primeiro capítulo, já se empreendeu esforço argumentativo para provar que, não obstante os princípios gerais da proteção de dados serem densificados nas leis gerais de proteção de dados, esses são decorrentes diretamente do direito constitucional à proteção de dados. Nesse sentido, já ponderou o Ministro Roberto Barroso: "Compartilhamento de dados pessoais para fins de produção de estatísticas somente será compatível com o direito à privacidade se:
1) a finalidade da pesquisa for precisamente delimitada;
2) o acesso for permitido na extensão mínima necessária para a realização dos seus objetivos;
3) forem adotados procedimentos de segurança suficientes para prevenir riscos de acesso desautorizado, vazamentos acidentais ou utilização indevida." BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387-MC Distrito Federal**. Plenário. Min. Rel. Rosa Weber. DJe em 12/11/2020. Voto do Min. Roberto Barroso, p. 5. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 06 ago. 2021.

[135] O seguinte trecho mostra a relevância da finalidade, adequação e necessidade: "A obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso de forma específica e precisa, e que os dados sejam adequados e necessários para essa finalidade. Com isso não seria compatível a armazenagem de dados reunidos, não anônimos, para fins indeterminados ou ainda indetermináveis. Todas as autoridades que reúnem dados pessoais para cumprir suas tarefas devem se restringir ao mínimo indispensável para alcançar seu objetivo

de dados pessoais serem vinculados a uma finalidade legítima e informados de forma clara ao titular dos dados. Por outro lado, o Decreto nº 10.046/2019 caminha em outro sentido. Por exemplo, o ato normativo determina que uma grande quantidade de dados – aqueles relativos ao compartilhamento amplo (art. 4º, I) – serão dispostos em "canais existentes para dados abertos" (art. 11), autorizando o acesso e processamento sem qualquer justificativa, tampouco conhecimento do titular.

Assim, ainda se constata evidente óbice ao cumprimento da autodeterminação informativa, ao passo que o diploma jurídico analisado não prevê ferramentas de acesso e controle dos dados pelos seus titulares. Dessa forma – além de não ser prevista a vinculação às intenções pelas quais os dados pessoais serão tratados pela Administração Pública em muitos casos – pelo que se observa da lógica do ato normativo, como regra, os cidadãos não terão conhecimento que seus dados estão sendo utilizados, o que impede qualquer forma de controle, como eventuais pedidos de retificação, por exemplo.

Em segundo, lembra-se que é corolário principiológico do direito fundamental à proteção de dados o mandamento de que os dados coletados devem ser os mínimos necessários para a consecução dos fins pretendidos (princípio da necessidade). Aqui, ao visualizar tal princípio em face do Decreto nº 10.046/2019, a problemática apresenta-se em ambivalência.

Primeiro que há como premissa referencial para a verificação do princípio da necessidade a clareza em relação da finalidade do tratamento, ponto já prejudicado em razão da disposição generalizada e abstrata de dados pessoais no Cadastro Base do Cidadão. Além disso, é preocupante a abrangência dos dados previstos no ato normativo, como é o caso das "bases temáticas" relativas a "atributos biométricos", como o formato da face e maneira de andar. Tal abrangência de dados pessoais – dos quais se pode inferir uma série de informações sensíveis dos cidadãos – coloca em dúvida a real necessidade da amplitude informacional prevista para o CBC.

Em terceiro, também se entende como ameaçado o princípio da segurança da informação. Nesse sentido, destaca-se a forma genérica e programática que o Decreto 10.046/2019 trata o tema, outorgando, sem maiores diretrizes, ao Comitê Central de

definido" (tradução livre: "Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.") BVerfGE – **Volkszählungsgesetz**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em 05 ago. 2021

Governança de Dados a competência para regular sobre o tema (art. 21, III)[136]. Acrescente-se a isso a fragilidade dos sistemas de segurança do Governo Federal brasileiro, sobre os quais, até o momento, somente em 2021, já se registraram 14.091 notificações e 3.641 incidentes[137]. Diante desse contexto, ainda pesa a seriedade e amplitude dos danos causados por incidentes de segurança em uma base de dados unificada, o que, aliás, foi um dos sólidos pontos argumentativos que afastaram a consolidação dessas bases em outros países (*National Data Center*, nos EUA e *SAFARI*, na França).

Sobre essa questão, ainda se pode afirmar que o Decreto nº 10.046/2019 e a previsão de uma base de dados unificada (CBC) guarda lógica completamente conflitante em relação ao importante conceito de "divisão informacional dos poderes", cunhada por Spiros Simitis[138] e reconhecida na decisão alemã de 1983[139]. A ideia é de que a íntima e perigosa relação entre poder e informação deve motivar o impedimento de uma "unidade informacional". Para tanto, compreende-se que só se deve outorgar o poder de coleta e tratamento de dados para órgão específico da Administração Pública (e somente para esse) quando estritamente necessário para a consecução de sua competência legal. Há, portanto, completa oposição entre essa concepção e a instituição do Cadastro Base do Cidadão[140].

Por fim, merece destaque o importante artigo de Gabriela Zanfir[141], que coloca como fator essencial para efetivação do direito à proteção de dados pessoais o que ela chama de "salvaguardas adequadas". No texto, essas salvaguardas são divididas em três eixos principais – de todos os quais depreendem-se omissões problemáticas do Decreto nº 10.046/2019: (i) o estabelecimento de direitos para os titulares dos dados, questão completamente ignorada pelo

---

[136] Em contraposição a essa escolhe normativa, tem-se a Lei nº 13.709/2018 (LGPD), que determina uma série de medidas importantes, como a comunicação à ANPD e aos titulares dos dados sobre os incidentes que possam acarretar riscos (art. 47) e a ideia de *privacy by design* (46, § 2º).

[137] CENTRO DE TRATAMETNO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **CTIRGov em Números:** Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. Disponível em: https://emnumeros.ctir.gov.br/. Acesso em 06 ago. 2021.

[138] Cf. SIMITIS, Spiros. Die informationelle Selbstbestimmung. Grundbedingung einer verfassungskonformen Informationsordnung. **Neue Juristische Wochenschrift**, v. 37, pp. 398-405, 1984.

[139] Nesse sentido: "Nas condições de uma tecnologia de processamento de dados em evolução, a distribuição constitucional de competências tem uma nova função." (tradução livre: "Unter den Bedingungen einer sich weiterentwickelnden Datenverarbeitungstechnologie komme der verfassungsrechtlichen Kompetenzverteilung eine neue Funktion zu.") BVerfGE – **Volkszählungsgesetz**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html. Acesso em 05 ago. 2021

[140] Cf. MARANHÃO, Juliano; CAMPOS, Ricardo. **A divisão informacional de Poderes e o Cadastro Base do Cidadão.** JOTA, 18/10/2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019#sdfootnote7anc. Acesso em 06 ago. 2021.

[141] ZANFIR, Gabriela. **Forgetting About Consent.** Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. (Eds.). **Reloading Data Protection Law:** Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2008. p. 237-257.

ato normativo, que, em lógica oposta à da LGPD[142], nem sequer cita os titulares dos dados pessoais, e tampouco cria mecanismos para acesso, controle e proteção de seus dados; (ii) o requisito de uma finalidade clara, a qual já se mostrou a deficiência do Decreto neste capítulo; e (iii) a previsão de mecanismos de responsabilização, também completamente ignorada pelo Decreto nº 10.046/2019, o que ainda é agravado em razão da formulação do CCGD, responsável pela resolução de conflitos e que, potencialmente, entra em embate de competência com a ANPD para impor as sanções dispostas na LGPD.

Assim, fica patente a existência de múltiplas violações ao devido processo informacional, o que implica, por sua vez, em ofensa direita ao direito fundamental à proteção de dados. Por último, no próximo tópico, passa-se a analisar o Decreto nº 10.046/2019 e a relação do princípio da proporcionalidade com a tutela dos dados pessoais, ponto que visa garantir um exame eficaz da legitimidade do processamento de dados pessoais pelo Poder Público.

3.3.3. PROPORCIONALIDADE: a necessidade do princípio na verificação da legitimidade do tratamento de dados pessoais

Como cediço no saber jurídico, há constantes desarmonias e embates entre os direitos fundamentais. Em sua seminal obra *"A era dos direitos"*[143], o influente jurista e filósofo Noberto Bobbio explica a questão a partir da constatação de que os direitos do homem pertencem a uma classe heterogênea, eis que não há apenas um fundamento que os sustente, mas vários, fato que, inevitavelmente, leva a desavenças internas ao próprio arcabouço normativo.

Por isso, faz-se necessário uma incessante busca pelo equilíbrio entre as garantias fundamentais, em consideração ao fato bem pontuado por Bobbio de que na "maioria das situações em que está em causa um direito do homem, ao contrário, ocorre que dois direitos igualmente fundamentais se enfrentem, e não se pode proteger incondicionalmente um deles sem tornar o outro inoperante"[144].

É exatamente desse anseio por equilíbrio que se funda o princípio da proporcionalidade. É dizer: a proporcionalidade deve ser guia principiológico que funcione como delimitador de

[142] O capítulo III da lei é destinado apenas para consolidação dos direitos do titular.
[143] BOBBIO, Norberto. **A Era dos Direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.
[144] Ibidem. p. 41.

fronteiras na interpretação e execução dos direitos fundamentais. Segundo Gilmar Mendes e Paulo Gonet[145], trata-se de princípio constitucional autônomo e geral do direito, integrado pelos seus seguintes elementos: (i) adequação – as medidas propostas devem ser aptas para alcançar o fim pretendido; (ii) necessidade – as medidas propostas devem ser o meio menos gravoso para consecução de seus objetivos; e (iii) proporcionalidade *strictu sensus* – rigorosa ponderação acerca das medidas propostas e dos direitos em tela.

No que diz respeito ao direito fundamental à proteção de dados e, mais especificamente, ao processamento de dados pessoais no Poder Público, Black e Stevens[146] tratam com maestria da relevância do princípio da proporcionalidade para a verificação da legitimidade do tratamento público de dados pessoais. Em primeiro, é premissa do trabalho dos autores o entendimento da proteção de dados pessoais como garantia de valor e interesse públicos. Como aprofundado neste trabalho (tópico 3.1.), se assim não fosse, poder-se-ia pressupor uma legitimidade abstrata e geral do tratamento de dados na Administração Pública, com fundamento constante no princípio da supremacia dos interesses públicos em detrimento dos privados.

Estruturada essa base, os acadêmicos propõem relevante teste[147], sintetizado no quadro a seguir:

---

[145] MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** São Paulo: Editora Saraiva, 2018.

[146] BLACK, Gillian; STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector**: The Critical Role Of Proportionality And The Public Interest. Scripted. Vol. 10, n. 1, 2013. Disponível em: https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest/ acesso em: 19 jul. 2021.

[147] A importância de tal teste vem se mostrando cada vez mais patente, exemplo disso foi a menção e utilização dele pelo Ministro Gilmar Mendes no julgamento de medida cautelar nos autos da ADPF nº 695/DF. Cf. BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695 Distrito Federal.** Rel. Min. Gilmar Mendes, decisão monocrática, DJe de 29/06/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 05 mai. 2021.

Quadro 4 – Teste de proporcionalidade de Gillian Black e Leslie Stevens

ETAPA 1: BASE LEGAL	ETAPA 2: QUALIFICAÇÃO DOS DADOS E RISCOS	ETAPA 3: PONDERAÇÃO	CONSOLIDAÇÃO ETAPA 3
O processamento atende a um objetivo legítimo (autorizado legalmente)?	Quais dados pessoais estão envolvidos neste processamento? São dados pessoais sensíveis? Quais são os riscos envolvidos em usá-los/divulgá-los e qual é a probabilidade de dano real ao indivíduo?	O interesse público no processamento supera o interesse privado do indivíduo e o interesse público mais amplo em proteger os dados pessoais?	O tratamento proposto dos dados pessoais é o meio menos intrusivo para atingir o objetivo do órgão público?
			O tratamento está em conformidade com a exigência de que os dados pessoais tratados não sejam excessivos?
			O processamento requer apenas a utilização de dados pessoais e não de dados pessoais sensíveis?
			A anonimização pode ser usada e, em caso afirmativo, a técnica proposta é considerada eficaz?
			O processamento proposto foi aprovado por um órgão de supervisão apropriado, quando relevante?
			Foi realizada uma avaliação do impacto da privacidade para avaliar e mitigar os riscos inerentes ao processamento em questão?
			Existe um interesse público identificável no processamento dos dados pessoais?
			Existe um interesse público identificável em fornecer ao público serviços relevantes?

Fonte: Sistematização própria, a partir do artigo "Enhancing Data Protection and Data Processing in the Public Sector"[148].

Voltando-se ao Decreto nº 10.046/2019, fica patente a sua insuficiente densificação normativa para verificação dos pontos em destaque no teste. Nesse sentido, percebe-se que a governança de compartilhamento de dados estabelecida e a instituição do Cadastro Base do

[148] Traduzido e adaptado de BLACK, Gillian; STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector**: The Critical Role Of Proportionality And The Public Interest. Scripted. Vol. 10, n. 1, 2013. Disponível em: https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest/ acesso em: 19 jul. 2021.

Cidadão estão envoltos de um plexo normativo que padece por sua generalidade e suas previsões abstratas, fato que compromete a verificação da proporcionalidade do tratamento de dados.

Mais do que isso, em face de alguns questionamentos do teste, pode-se vislumbrar respostas com peso obstativo para a legitimidade do tratamento de dados pessoais disposto no Decreto nº 10.046/2019, como é o caso do compartilhamento de dados sensíveis[149], a excessividade de dados coletados e a ausência de mecanismos de avaliação de impactos sobre a privacidade.

Dessa forma, conclui-se o terceiro e último ponto deste exame de compatibilidade entre o ato normativo analisado e o direito fundamental à proteção de dados. Como nas outras oportunidades, no presente tópico, ficou clara a deficiência das disposições do diploma jurídica quando analisados à luz das lições jurídicas mais atualizadas sobre a tutela dos dados pessoais.

[149] Reforça-se, aqui, que a Lei nº 13.709/2018 (LGPD) conceitua como dado sensível o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II). Nesse sentido, percebe-se que a amplitude de dados prevista no Decreto nº 10.046/2019 alcança o conceito de dados sensíveis. Como é o caso da própria inclusão da "base temática" de "atributos biométricos" no Cadastro Base do Cidadão.

CONSIDERAÇÕES FINAIS

É bem verdade que o incremento das tecnologias de informação e comunicação acarretou em uma série de vantagens para a sociedade, tais quais a maior facilidade ao acesso à informação e a diluição de várias barreiras de comunicabilidade. Contudo, não há de se olvidar que, de uma forma, o uso generalizado dessas tecnologias implicou na disponibilização de um massivo "rastro" de dados pessoais e, de outra maneira, o desenvolvimento tecnológico também acarretou em um relevante progresso da capacidade de processamento de dados. Tal conjuntura configurou novos riscos à privacidade e a outros direitos fundamentais e, consequentemente, conferiu caráter de urgência a uma adequada tutela dos dados pessoais.

Dado tal contexto, buscou-se, preliminarmente, expor o relevante processo histórico que perfez caminho desde a formulação do direito à privacidade até o reconhecimento de um direito fundamental autônomo à proteção de dados. Para além disso, demonstrou-se a relevância das discussões acerca dos riscos a um importante conjunto de direitos fundamentais decorrentes do tratamento de dados dentro do Poder Público. Como foi nos casos do *National Data Center* (EUA), *SAFARI* (França) e na decisão sobre o censo demográfico (Alemanhã).

Aliás – o que de forma alguma implica em um entendimento de inferioridade do rico debate sobre os riscos de tratamento de dados em iniciativas privadas –, o processamento de dados no setor público foi o recorte de pesquisa selecionado. Mais especificamente, o presente trabalho buscou desenvolver o conceito e as principais lições dogmáticas do direito fundamental à proteção de dados para, a partir de então, examinar o Decreto nº 10.046, de 2019, que dispõe "sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados".

Para tanto, foram apresentados importantes aprendizados do direito alemão, em razão de sua relevância na gênese e desenvolvimento do processo de constitucionalização da tutela de dados pessoais. Nesse sentido, adotou-se técnica metodológica de expor decisões centrais do Tribunal Constitucional Federal alemão (BVerfG) e, a partir delas, analisar contornos importantes do direito fundamental à proteção de dados.

Assim, em um primeiro ponto, foi analisada a formulação no Judiciário germânico do direito geral de personalidade, assim como sua função de atualização da tutela da personalidade humana, caminho necessário para a formulação do próprio direito à autodeterminação informativa, na decisão de 1983 sobre o censo demográfico. O segundo ponto tratou exatamente

desta emblemática decisão, explorando as razões tecidas pela Suprema alemã e aprofundando-se oportunamente nos princípios gerais da proteção de dados pessoais. Por último, buscou-se examinar a decisão alemã que reconheceu o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais. Sobre o julgado, aproveitou-se as célebres reflexões do ex-ministro do Tribunal Constitucional Federal alemão e especialista em proteção de dados, Wolfgang Hoffman-Riem[150], para adentrar nas dimensões objetiva e subjetiva do direito fundamental à proteção de dados pessoais.

Voltando-se para o contexto brasileiro, buscou-se examinar as lições doutrinárias nacionais, expondo longo trajeto, desde estudos que relacionavam a questão dos dados pessoais a disposições constitucionais específicas (direito à privacidade e inviolabilidade das comunicações – art. 5º, X e XII, CF/88) até o entendimento doutrinário de um direito implícito e autônomo fundamental à proteção de dados na Constituição, reconhecido mediante hermenêutica constitucional sistêmica, com enfoque à dignidade da pessoa humana, ao livre desenvolvimento da personalidade, ao direito geral à liberdade e à própria previsão do *habeas data*.

Bem assim, explorou-se o desenvolvimento jurisprudencial da matéria no Supremo Tribunal Federal. Em vista de fornecer uma visão geral sobre como a corte tratou o direito fundamental à proteção de dados, apresentou-se quatro decisões, que vão desde o entendimento de que os dados protegidos são apenas os que estão em fluxo (MS nº 21.729/DF e RE nº 418.416/SC), passando por decisão de "meio do caminho" que reconheceu o conceito de dados pessoais em espectro ampliado (RE nº 673.707/MG), até, finalmente, a decisão que reconheceu o direito fundamental e autônomo à proteção de dados pessoais. Além disso, por último, visou-se já construir uma ponte com o último capítulo, examinando os dois processos do Supremo que tratam sobre o Decreto nº 10.046/2019 (ADPF nº 695/DF e ADI nº 6.649/DF).

Por fim, após o desenvolvimento jurídico acerca de um direito constitucional e autônomo à proteção de dados nos capítulos anteriores, partiu-se para apresentação e análise do Decreto nº 10.046/2019. Antes disso, todavia, destinou-se atenção especial para as peculiaridades da proteção de dados pessoais no setor público, ressaltando seu valor transindividual e sua imprescindibilidade para o regime democrático.

Após exame minucioso dos principais dispositivos do Decreto nº 10.046/2019, finalmente, passou-se a analisar – o que se entendeu ser – os principais pontos de desarmonia

[150] HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, pp. 54-57, jul-ago 2015.

do diploma com o direito fundamental desenvolvido. Nesse viés, o primeiro ponto conflitante foi a supervalorização da natureza dos dados pessoais conferida pelo ato normativo. Em sentido contrário, a partir de Helen Nissenbaum como marco teórico[151], entende-se que se deve proteger os dados pessoais em função de cada contexto específico de tratamento e não somente a partir de uma análise ontológica dos dados.

Sobre o segundo ponto de incompatibilidade, destaca-se a posição do devido processo informacional como decorrência automática e inevitável da garantia constitucional de tutela dos dados pessoais, importando em uma série de regras protetivas a serem seguidas no processamento de dados pessoais. Mostrou-se, portanto, que Decreto nº 10.046/2019 padece por inconstitucionalidade, também, em razão de violações claras a esse devido processo, tais quais o desrespeito a princípios gerais da proteção de dados pessoais, omissão acerca dos direitos do titular de dados e ausência da previsão de meios de responsabilização.

O terceiro ponto de inconstitucionalidade do Decreto e último ponto do trabalho tratou de ressaltar a importância da proporcionalidade como ferramenta necessária para verificação da legitimidade do tratamento de dados no Poder Público. Densificando a questão, apresentou-se o teste de proporcionalidade Black e Stevens[152]. Em face do teste, mais uma vez o ato normativo mostrou-se falho: a generalidade e as previsões demasiadamente abstratas do diploma impedem uma análise de proporcionalidade válida.

Por fim, entende-se que a pergunta que guiou este trabalho pode ser respondida com certa segurança no sentido da inconstitucionalidade do Decreto nº 10.046/2019, tese que buscou respaldo nas mais modernas lições sobre o direito fundamental à proteção de dados pessoais. Nesse sentido, entende-se que a ideia de centralização de dados no Cadastro Base do Cidadão por si mesma já antiquada, tendo em vista as discussões internacionais e o afastamento de propostas parecidas nas décadas de 1960 e 1970. E também pela contrariedade à assertiva posição de Spiros Smiths[153] sobre "divisão informacional dos poderes", que rechaça qualquer forma de "unidade informacional" em nome da segurança e proteção dos dados pessoais.

---

[151] NISSENBAUM, Helen. Privacy as Contextual Integrity. **Washington Law Review**, v. 79, pp. 101-139. 2004. Disponível em: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf. Acesso em 31 jul. 2021.

[152] BLACK, Gillian; STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector**: The Critical Role Of Proportionality And The Public Interest. Scripted. Vol. 10, n. 1, 2013. Disponível em: https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest/ acesso em: 19 jul. 2021.

[153] SIMITIS, Spiros. Die informationelle Selbstbestimmung. Grundbedingung einer verfassungskonformen Informationsordnung. **Neue Juristische Wochenschrift**, v. 37, pp. 398-405, 1984.

Como se não bastasse, o ato normativo ainda mostra numerosas incongruências com a lógica da proteção de dados, ignorando uma série de disposições normativas consideradas como base essencial para salvaguarda dos direitos do titular de dados.

Diante do todo, acredita-se que o tratamento de dados pessoais na Administração Pública e seus frutos devem ser perseguidos e regulados de outra forma para, assim, buscar alcance a ideia de Simson Garfinkel[154] apresentada na introdução – de viabilidade de um "desenvolvimento sustentável", que coloca em harmonia o valor da privacidade com o progresso tecnológico.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil:** interceptações, quebras de sigilo, infiltrações e seus limites constitucionais**.** São Paulo: InternetLab, 2017.

ASSMANN, JHONATA. **O Direito à Autodeterminação Informativa no Direito Germânico e Brasileiro.** Orientador: Airton Lisle Cerqueira L. Seelaender. 2014. 65 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: http://150.162.242.35/bitstream/handle/123456789/117169/Jhonata%20Assmann%20TCC%20pdfa.pdf?sequence=1&isAllowed=y. Acesso em: 02 jun. 2021.

BENNET, Colin; ODURO-MARFO, Smith. **Privacy, Voter Surveillance, and Democratic Engagement:** Challenges for Data Protection Authorities. International Conference of Data Protection and Privacy Commissioners (ICDPPC), Greater Victoria, 2019.

BIONI, Bruno; MARTINS, Pedro. **Devido processo informacional:** um salto teórico-dogmático necessário? JOTA, 15 jul. 2020. Disponível em: https://www.jota.info/opiniao-e-

[154] GARFINKEL, Simson. **Database Nation: the death of privacy in the 21th Century.** California: O'Reilly Media, 2000. p. 15.

analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020. Acesso em 05 ago. 2021.

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

BLACK, Gillian; STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector**: The Critical Role Of Proportionality And The Public Interest. Scripted. Vol. 10, n. 1, 2013. Disponível em: https://script-ed.org/article/enhancing-data-protection-data-processing-public-sector-critical-role-proportionality-public-interest/ acesso em: 19 jul. 2021.

BOBBIO, Norberto. **A Era dos Direitos**. Trad. Carlos Nelson Coutinho. Rio de Janeiro: Elsevier, 2004.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Decreto nº 10.046**, 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 03 mai. 2021.

BRASIL. **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: 03 jun. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387 Distrito Federal.** Rel. Min. Rosa Weber, Plenário, DJe de 12/11/2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 24 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.649 Distrito Federal**. Rel. Min. Gilmar Mendes. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238. Acesso em 03 mai. 2021.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 695 Distrito Federal.** Rel. Min. Gilmar Mendes, decisão monocrática, DJe de 29/06/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em 05 mai. 2021.

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança nº 21.729 Distrito Federal.** Rel. Min. Marco Aurélio, Red. do Acórdão Min. Néri da Silveira, Plenário, DJ de 19/10/2001. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 Acesso em 15 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 418.416 Santa Catarina.** Rel. Min. Sepúlveda Pertence, Plenário, DJ de 19/12/2006. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790. Acesso em 15 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 673.707 Minas Gerais.** Rel. Min. Luiz Fux, Plenário, DJe 30/09/2015. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=307831711&ext=.pdf. Acesso em: 26 mar. 2021.

BRASIL. **Proposta de Emenda à Constituição nº 17**, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em 27 mar. 2021.

CANOTILHO, José Joaquim Gomes; MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; STRECK, Lênio Luiz. **Comentários à Constituição do Brasil.** 1. ed. São Paulo: Saraiva, 2013.

CENTRO DE TRATAMETNO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **CTIRGov em Números:** Estatísticas resultantes do trabalho de detecção,

triagem, análise e resposta a incidentes cibernéticos. Disponível em: https://emnumeros.ctir.gov.br/. Acesso em 06 ago. 2021.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS. **Regras para Compartilhamento de Dados.** 4 mai. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/regras-de-compartilhamento_v1-0.pdf. Acesso em 31 jul. 2021.

CONCIL OF EUROPE. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, 28 jan. 1981. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37. Acesso em 20 mar. 2021.

CONFESSORE, Nicholas. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. **New York Times.** New York, 4 abr. 2018 Disponível em: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html. Acesso em: 13 mar. 2021.

DÖHMANN, Indra Spiecker genannt. **A proteção de dados pessoais sob o regulamento geral**. *In:* DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 97-113.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** São Paulo: Renovar, 2006.

DONEDA, Danilo. **Panorama Histórico da Proteção de Dados Pessoais**. *In:* DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 3-20.

ERD, Rainer. Bundesverfassungsgericht versus Politik: Eine Kommentierende Dokumentation Der Jüngsten Entscheidungen Zu Drei Sicherheitsgesetzen. **Kritische Justiz**, vol. 41, no. 2, 2008, pp. 118–133. JSTOR, www.jstor.org/stable/24238877. Acesso em 16 jun 2021.

FERRAZ JR., Tercio Sampaio. Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, p. 439-459, 1993.

FRAZÃO, Ana. **Proteção de dados e democracia:** a ameaça da manipulação informacional e digital. In: FRANCOSKI, Denise de Souza Luiz; TASSO, Fernando Antônio. **A Lei Geral de Proteção de Dados Pessoais:** aspectos práticos e teóricos relevantes no setor público e privado. São Paula: Revista dos Tribunais. 2021.

GARFINKEL, Simson. **Database Nation:** the death of privacy in the 21th Century**.** California: O'Reilly Media, 2000.

GASIOLA, Gustavo Gil; MACHADO, Diego; MENDES, Laura Schertel. A administração pública entre transparência e proteção de dados. **Revista do Direito do Consumidor.** São Paulo: RT. vol. 135/2021. p. 191. Maio-Jun/2021.

GUIMÓN, Pablo. "O 'Brexit' não teria acontecido sem a Cambridge Analytica". **EL PAÍS.** Londres, 16 mar. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/26/internacional/1522058765_703094.html. Acesso em: 13 mar. 2021.

HILL, Kashmir. Wrongfully Accused by an Algorithm. **New York Times.** New York, 24 jun. 2020. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Acesso em 13 mar. 2021.

HOFFMANN-RIEM, Wolfgang. Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información. **RDU**, Porto Alegre, Volume 12, n. 64, 2015, p. 40-61, jul-ago 2015.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data Protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. **Computer Law And Security Review**, Kassel, n. 25, p.115-122, 2009.

JUSTINO, Luiz Carlos da Costa. “QUAL FACÇÃO, VAGABUNDO?”: O violoncelista inocente que ficou cinco dias preso. **Revista Piauí**, Edição 169, out. 2020. Disponível em: https://piaui.folha.uol.com.br/materia/qual-faccao-vagabundo/. Acesso em: 13 mar. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet.** São Paulo: Saraiva, 2012. p. 122.

LONG, Clarisa. **Privacy and Pandemics**. In: PISTOR, Katharina. **Law in the time of COVID-19**. Columbia Law School Books, 2020. p. 92.

MARANHÃO, Juliano; CAMPOS, Ricardo. **A divisão informacional de Poderes e o Cadastro Base do Cidadão.** JOTA, 18/10/2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019#sdfootnote7anc. Acesso em 06 ago. 2021.

MAYER-SCHÖNBERGER, Viktor. **Generational development of data protection in Europe**. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and privacy: the new landscape.** Cambridge: The Mit Press, 1997.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional.** São Paulo: Editora Saraiva, 2018.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. **Pensar**, Fortaleza, v. 25, n. 4, p. 11, out./dez. 2020.

MENDES, Laura Schertel; BIONI, Bruno. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor.** Vol. 124. Ano 28. São Paulo: Editora RT, p. 157-180, jul-ago 2019.

MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. **Revista Direitos Fundamentais & Justiça**, a. 12, n. 39, pp. 185-216, jul./dez. 2018.

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

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais**: rumo a um direito fundamental autônomo. *In:* DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 61-71.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. **Revista Jurídica Luso-Brasileira – RJLB**, Ano 5, nº 1, pp. 781-809, 2019.

NISSENBAUM, Helen. Privacy as Contextual Integrity. **Washington Law Review**, v. 79, pp. 101-139. 2004. Disponível em: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf. Acesso em 31 jul. 2021.
Organisation for Economic Co-operation and Development – OCDE. **The Path to Becoming a Data-Driven Public Sector**. OECD Publishing: Paris, 2019.

PAULUZE, Thaiza. Foto em delegacia faz jovem negro ser acusado 9 vezes e preso duas vezes por roubos que não cometeu. **Folha de São Paulo**. São Paulo 2 jan. 2021 Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/01/foto-em-delegacia-faz-jovem-negro-ser-acusado-9-vezes-e-preso-duas-por-roubos-que-nao-cometeu.shtml. Acesso em: 13 mar. 2021.

QUEIROZ, Rafael Mafei Rabelo; PONCE, Paula Pedigoni. Tercio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado. **Internet & Sociedade**, São Paulo, n. 1, v. 1, p. 64-90, 2020.

REGAN, Priscilla. **Legislating Privacy**: Technology, Social Values and Public Policy. Chapel Hill: University of North Carolina Press.

RUTH, Gavison. Privacy and the Limits of the Law. **The Yale Law Journal**. vol. 89, no 3, p. 455, jan/1980.

SARLET, Ingo Wolfgang. **Fundamentos constitucionais**: o direito fundamental à proteção de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 21-61.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 14, n. 42, pp. 179-218, jan./jun. 2020. Disponível em: https://dspace.almg.gov.br/bitstream/11037/38102/1/Ingo%20Wolfgang%20Sarlet.pdf. Acesso em: 11/03/2021.

SARMENTO. Daniel. **Supremacia do interesse público?** As colisões entre direitos fundamentais e interesses da coletividade. In: ARAGÃO, Alexandre Santos de; MARQUES NETO, Floriano Azevedo. **Direito administrativo e seus novos paradigmas.** Belo Horizonte: Fórum, 2008. p. 97-143.

SCHWABE, Jürgen; MARTINS, Leonardo. Decisão do Tribunal Constitucional alemão de 1983. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevideo: Konrad Adenauer Stiftung, 2005, pp. 233-245. Disponível em: http://www.kas.de/wf/doc/kas_7738-544-1-30.pdf. Acesso em: 11/03/2021.

SIMITIS, Spiros. Die informationelle Selbstbestimmung. Grundbedingung einer verfassungskonformen Informationsordnung. **Neue Juristische Wochenschrift**, v. 37, pp. 398-405, 1984.

SOLOVE, Daniel. **Understanding Privacy.** Cambridge: Harvard University Press, 2008.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. IV, n. 5, pp. 193-220, 1890.

WESTIN, Alan Furman. **Democracy and Freedom**. New York: IG Publishing. 1968. p. 45-46. (ebook)

WILMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. *In:* DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, pp. 271-288.

ZANFIR, Gabriela. **Forgetting About Consent.** Why The Focus Should Be On "Suitable Safeguards" in Data Protection Law. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul. (Eds.). **Reloading Data Protection Law:** Multidisciplinary Insights and Contemporary Challenges. London: Springer, 2008. p. 237-257.

ZANINI, Leonardo Estevam de Assis. A proteção dos direitos da personalidade na Alemanha. **Revista Direitos Culturais**, Santo Ângelo-RS, v. 14, n. 33, p. 135-158, 2019.