© ***Cadernos de Dereito Actual*** Nº 18. Núm. Ordinario (2022), pp. 326-343
·ISSN 2340-860X - ·ISSNe 2386-5229

Compartilhamento e tratamento de dados pessoais pelo setor público no Brasil: uma análise do Decreto n. 10.046/2019

Sharing and processing of personal data by the public administration in Brazil: analyse of Decree n. 10,046/2019

Gilson Delgado Miranda[1]
Erika Doria[2]
Liliane Mageste Barbosa[3]
Pontifícia Universidade Católica de São Paulo

Resumo: Diante de um contexto de avanços na tecnologia da informação, os quais impactam em diversos aspectos da vida em sociedade, o presente artigo objetiva examinar o tratamento e o compartilhamento de dados pessoais pela Administração Pública no Brasil, feitos sob a justificativa da necessidade de elaboração e execução de políticas públicas. A análise será feita em cotejo com o direito fundamental à proteção de dados pessoais e o arquétipo protetivo trazido pela novel legislação de proteção de dados brasileira. Os pontos levantados permitirão demonstrar incompatibilidades do Decreto n. 10.046/2019 com a Constituição da República de 1988 e com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018).

Palavras-chave: dados pessoais, tratamento, compartilhamento, políticas públicas.

Abstract: In the context of advances in information technology, which impact on several aspects of life in society, this article aims to analyze the processing and sharing of personal data by the Public Administration, under the justification of the need to prepare and implement public policies. The analysis will be performed considering the fundamental right to the protection of personal data and the protective archetype resulting from the new Brazilian legislation regarding data protection. The points raised will highlight incompatibilities of Decree No.

[1] Doutor em Direito pela Pontifícia Universidade Católica de São Paulo (1988). Mestre em Direito pela Pontifícia Universidade Católica de São Paulo (1998). Professor assistente-doutor da Pontifícia Universidade Católica de São Paulo. Vice-diretor da Escola Paulista da Magistratura - EPM, eleito para o biênio 2022/2023. Desembargador no Tribunal de Justiça do Estado de São Paulo.

[2] Especialista em Direito Constitucional pela Pontifícia Universidade Católica de São Paulo / Coordenadoria Geral de Especialização, Aperfeiçoamento e Extensão (COGEAE). Mestranda em Direito do Estado pela Pontifícia Universidade Católica de São Paulo (PUC-SP). Defensora Pública do Estado de São Paulo.

[3] Mestranda em Direitos Difusos e Coletivos pela PUC-SP. Defensora Pública do Estado de São Paulo.

Recibido: 15/01/2022
Aceptado: 20/06/2022

10,046/2019 with the Constitution of the Republic of 1988 and the General Data Protection Law (Law no. 13,709/2018).

Keywords: personal data, processing, sharing, public policies.

1. Introdução

Com a ascensão do Estado de Bem-Estar Social, a partir do século XX, principalmente, o poder público adquiriu novas responsabilidades relacionadas à promoção de direitos fundamentais, as quais exigem uma atuação positiva voltada ao planejamento, organização, coordenação e execução de políticas públicas que assegurem à população a educação, a saúde, o lazer e demais direitos. Para o adequado dimensionamento dessas medidas, imprescindível a realização de censos e coleta dos mais variados dados, o que garantirá sua eficácia e economicidade, notadamente, em um cenário de recursos limitados.

O período inaugurado pelo século XX também se caracteriza pela contínua evolução das tecnologias da informação, que passaram a permitir o tratamento de dados de maneira cada vez mais veloz, sofisticada e personalizada, atendendo às necessidades de diversos setores.[4] Observa-se que os dados pessoais adquiriram manifesta relevância no contexto da sociedade contemporânea, sendo indiscutível que o seu uso propicia o desenvolvimento econômico e social. Especificamente na esfera pública é notável a importância de tais tecnologias em diversos campos, como o da elaboração de políticas públicas e o da segurança nacional.

No entanto, não se pode olvidar que o uso das informações veiculadas pelos dados pessoais possibilita o acesso a diversos aspectos da individualidade.[5] Tal conjuntura é agravada pelo fato de, muitas vezes, o fornecimento desses dados ser condição *sine qua non* para a utilização de bens e serviços, situando o titular em uma posição de maior vulnerabilidade. A constatação dessas circunstâncias inaugurou uma nova preocupação para o Direito, no sentido de corrigir (ou, ao menos, atenuar) as distorções entre as partes de uma relação jurídica que envolva o tráfego de informações.

Assim, a partir da percepção de que o tratamento de dados pessoais não deve ocorrer de forma indiscriminada, diversos ordenamentos jurídicos passaram a se debruçar sobre o assunto, criando sistemas normativos que informam balizas para uma boa governança e boa procedimentalização na atividade de tratamento de dados.

Historicamente, a doutrina considera que a primeira norma sobre o tema teria sido promulgada em 1970 no Estado de Hesse, na Alemanha. Desde então, a matéria, fruto de intensas discussões, ganhou institutos e conceitos próprios, a exemplo da

[4] No presente artigo, os autores destacam as tecnologias diretamente voltadas ao tratamento de dados pessoais, que se tornaram mais relevantes no século XX. Contudo, não se olvida a célebre obra de Samuel Warren e Louis Brandeis, "*The Right to Privacy*", de 1890, em que se consolidaram bases doutrinárias para o desenho do direito fundamental à privacidade, como o direito de ser deixado só ("*right to be let alone*"). Ressalta-se que os autores demonstraram o vínculo entre a privacidade e o avanço tecnológico, no sentido de que quanto mais avançada a tecnologia, maior será a facilidade de invadir o espaço privado dos cidadãos. WARREN, S. BRANDEIS, L. "The right to privacy", *Harvard Law Review*, v. IV, n. 5, 1890 Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 19 set. 21.

[5] Diante de tecnologias que realizam o agrupamento de dados e a criação de perfis dos titulares (*profiling*), entende-se que o fornecimento de qualquer dado poderá vir a afetar a individualidade, visto que o cruzamento de informações possibilita o acesso a circunstâncias que, eventualmente, o indivíduo tenha desejado não divulgar a um determinado agente.

necessidade de se estabelecer direitos aos cidadãos, facilitar o fluxo de informações entre países e mitigar os riscos advindos das operações de tratamento de dados. Hoje, a regulamentação normativa está presente em cerca 140 países.[6]

No Brasil, o arcabouço normativo abrange normas como o Código de Defesa do Consumidor (Lei n. 8078/1990), a Lei do Cadastro Positivo (Lei n. 12.414/2011), a Lei de Acesso à Informação (Lei n. 12.527/2011), o Marco Civil da Internet (Lei n. 13.965/2014) e, mais diretamente, a novel Lei Geral de Proteção de Dados (Lei n. 13.709/2018), que entrou em vigor a partir de setembro de 2020. Outrossim, recentemente, a Emenda Constitucional n. 115/2022 foi aprovada para incluir no rol de direitos fundamentais do artigo 5ºo direito à proteção dos dados pessoais.7

Diante desse contexto, o presente artigo visa analisar um aspecto específico do tratamento de dados pessoais, consistente no compartilhamento destes na esfera pública, sob a justificativa de necessidade de elaboração e execução de políticas públicas. Também será objeto de estudo a legalidade e constitucionalidade do Decreto n. 10.046/2019, que, além de tratar do compartilhamento de dados no âmbito da administração pública federal, institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Buscar-se-á demonstrar quais são os limites a serem observados pelas instituições inseridas no primeiro setor, tendo em vista a fundamentalidade do direito à proteção de dados pessoais, cuja estrutura se encontra prevista na Lei n. 13.709/2018.

Justifica-se a pesquisa em decorrência da relevância do sopesamento de valores como, de um lado, a eficiência na gestão pública e o desenvolvimento social e, de outro, a proteção de dados como um direito fundamental que, apesar de autônomo[8], encontra-se interrelacionado à intimidade, à privacidade, ao livre desenvolvimento da personalidade, dentre outros direitos fundamentais correlatos.

A partir da metodologia dedutiva, serão apresentados conceitos hábeis a fundamentar a tentativa de conciliação entre a proteção de dados pessoais e o seu compartilhamento entre esferas estatais. O trabalho, amparado no estudo doutrinário, normativo e jurisprudencial, será dividido nos seguintes subtemas: inicialmente, versará sobre o enquadramento constitucional do direito à proteção de dados, indicando seus fundamentos. Em seguida, será delineado o cenário evolutivo da proteção de dados em face do poder público, oportunidade em que reflexões sobre o direito comparado serão de grande valia. Posteriormente, o artigo abordará o sistema normativo brasileiro acerca da temática, com enfoque voltado ao conteúdo da regulamentação da Lei n. 13.709/2018 sobre o setor público. Por fim, será examinado como o arquétipo normativo em comento permite o compartilhamento de dados pessoais entre diversos atores do setor público. À luz da principiologia contida na mencionada lei, serão realizados apontamentos sobre certos desvios previstos no Decreto n. 10.046/2019.

2. Proteção de dados pessoais como direito fundamental

O avanço da tecnologia provocou o surgimento de complexas redes de tratamento de dados pessoais, as quais, dotadas de inteligência artificial, são altamente eficientes. Observa-se que o desenvolvimento tecnológico, não raro, afeta a transparência que deveria existir na referida atividade, de modo que os titulares

---

[6] DONEDA, D. C. M. "Panorama histórico da proteção de dados pessoais", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, p. 3 (notas de rodapé 01 e 02).

7 Estabelece a Constituição Federal que: "*Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)*"

[8] Como já mencionado, esse direito foi recentemente incorporado ao rol de direitos fundamentais pela Emenda Constitucional n. 115/2022.

nem sempre são cientificados sobre a utilização de seus dados. Não por outro motivo, Frank Pasquale cunhou a expressão "caixa preta dos algoritmos", a indicar que a automatização na tomada de decisões a partir de processos obscuros pode viabilizar abusos sem que os cidadãos os percebam.[9]

Ademais, tornou-se praticamente inviável optar por não divulgar dados pessoais, uma vez que a coleta destes, muitas vezes, condiciona o próprio exercício regular de direitos. Virginia Eubanks pondera, por exemplo, que as pessoas que mais necessitam do amparo das políticas públicas para alcançar o mínimo existencial têm suas vidas devassadas pela coleta excessiva de informações. Paradoxalmente, a coleta massiva de dados para promoção de políticas públicas pode aprofundar as desigualdades sociais.[10]

Tais condições sociais geram profundas disparidades entre os diversos agentes controladores de dados e os indivíduos, incrementando a vulnerabilidade destes nas relações jurídicas. Consequentemente, verifica-se a urgência da tutela da pessoa pelo Direito no tocante ao tratamento de seus dados pessoais.

O direito à proteção de dados pessoais não se encontrava expressamente positivado na Constituição da República Federativa do Brasil de 1988, situação que se alterou após a recente promulgação da Emenda Constitucional n. 115/2022, responsável por positivar o direito fundamental à proteção de dados pessoais.

Merece destaque o fato de a justificativa que acompanhou a apresentação da Proposta de Emenda Constitucional n. 19/2019 reconhecer os impactos e os novos desafios apresentados diante da evolução tecnológica, sublinhando que "*o assunto, cada vez mais, na Era Informacional, representa riscos às liberdades e às garantias individuais dos cidadãos*"[11]. Assim, na esteira de outros países como Portugal, Chile,

---

[9] Segundo o autor, "*The term "black box" is a useful metaphor for doing so, given its own dual meaning. It can refer to a recording device, like the data-monitoring systems in planes, trains, and cars. Or it can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we can not tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences*.". Tradução livre: "*O termo "caixa preta" é uma metáfora útil, dado seu próprio duplo significado. Ele pode se referir a um dispositivo de gravação, como os sistemas de monitoramento de dados em aviões, trens e carros. Ou pode significar um sistema cujo funcionamento é misterioso; podemos observar suas entradas e saídas, mas não podemos dizer como um se torna o outro. Enfrentamos esses dois significados: empresas e governo nos acompanham de modo detalhado, e não temos controle ou ideia de como essas informações são compartilhadas, usadas e as consequências advindas deste uso*". PASQUALE, F. *The black box society*, Cambrigde, Massachusetts, London, England: Harvard University Press, 2015, Versão eletrônica do Kindle.

[10] Segundo a autora: "*Marginalized groups face higher levels of data collection when they access public benefits, walk through highly policed neighborhoods, enter the health-care system, or cross national borders. That data acts to reinforce their marginality when it is used to target them for suspicion and extra scrutiny. Those groups seen as undeserving are singled out for punitive public policy and more intense surveillance, and the cycle begins again. It is a kind of collective red-flagging, a feedback loop of Injustice*." Tradução livre: "*Grupos marginalizados enfrentam níveis mais elevados de coleta de dados quando acessam benefícios públicos, caminham por bairros altamente policiados, entram no sistema de saúde ou cruzam fronteiras nacionais. Esses dados atuam para reforçar sua marginalidade quando são usados para alcançá-los por suspeita. Esses grupos vistos como indignos são apontados para políticas públicas punitivas e vigilância mais intensa, e o ciclo recomeça. É uma espécie de coletiva de sinalização vermelha, um ciclo vicioso de injustiça.*" EUBANKS, V. *Automating inequality*. New York: St. Martin's Publishing Group: 2018, Versão eletrônica do Kindle.

[11] BRASIL, Senado Federal. Justificação à proposta de Emenda Constitucional n. 17/2019, proposta em 12.03.2019, de lavra do Senador Eduardo Gomes. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em

Estônia e Polônia, identificou-se a necessidade de tornar a proteção de dados um direito fundamental expresso.

Contudo, mesmo antes da aprovação da apontada Emenda Constitucional, a partir do referendo, pelo Pleno do Supremo Tribunal Federal, da medida cautelar concedida pela Ministra Rosa Weber na Ação Direta de Inconstitucionalidade n. 6387/DF, restou fortemente consolidado o entendimento segundo o qual se fazia necessária uma interpretação atualizadora da Constituição da República, a fim de conformar o contexto constitucional à realidade imposta pelas inovações tecnológicas que surgiram após 1988.[12]

Cumpre destacar, de acordo com o voto da Ministra Relatora, que o amparo constitucional aos dados pessoais decorreria do fato de integrarem "*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).*"[13]

O Ministro Gilmar Mendes, por sua vez, identificou que o direito fundamental à proteção de dados pessoais advinha de uma leitura integrada de diversos dispositivos constitucionais, dentre os quais a dignidade da pessoa humana e a proteção constitucional da intimidade (art. 5º, inciso X, da CF/88), tratando-se de consequência da necessária atualização da força normativa da Constituição e seus compromissos políticos. O Ministro citou, ainda, a garantia fundamental ao *Habeas Data*, classificando-o como mecanismo apto a tutelar o direito à autodeterminação informativa.[14]

Infere-se que o reconhecimento de um direito fundamental à proteção de dados pessoais decorreu, mesmo antes de sua positivação no artigo 5º, inciso LXXIX, da Constituição Federal, de um lado, da interpretação sistemática da Constituição da República[15] e, de outro, da constatação de que a realidade deve influenciar diretamente o processo interpretativo das normas constitucionais.[16]

Considera-se, então, que a construção jurídica que já sustentava a autonomia de um direito fundamental à proteção de dados pessoais afigurou-se plenamente acertada, por ter assegurado sua guarida específica enquanto inexistia previsão constitucional expressa.

Imperioso ressaltar que, anteriormente à promulgação da Emenda Constitucional n. 115/2022, a percepção da proteção dos dados pessoais como um direito fundamental autônomo era fruto da constatação da insuficiência de outros

---

23.02.2022. Como já mencionado, referida proposta foi aprovada como Emenda Constitucional de n. 115/2022.

[12] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade: ADI 6387/DF. Tribunal Pleno. Relatora: Ministra Rosa Weber. Julgamento: 07/05/2020, p.20 Publicação: 12/11/2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 18 set. 2021.

[13] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade: ADI 6387/DF. Tribunal Pleno. Relatora: Ministra Rosa Weber. Julgamento: 07/05/2020, p. 21 Publicação: 12/11/2020. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 18 set. 2021.

[14] BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade: ADI 6387/DF. Tribunal Pleno. Relatora: Ministra Rosa Weber. Julgamento: 07/05/2020. Publicação: 12/11/2020, p 98. Disponível em: https://jurisprudencia.stf.jus.br/pages/search?classeNumeroIncidente=%22ADI%206387%22&base=acordaos&sinonimo=true&plural=true&page=1&pageSize=10&sort=_score&sortBy=desc&isAdvanced=true. Acesso em 18 set. 2021.

[15] MENDES, L. S. F. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Versão eletrônica do Kindle.

[16] BARROSO, L. R. *Curso de direito constitucional contemporâneo*: os conceitos fundamentais e a construção do novo modelo. 3ª ed. São Paulo: Saraiva, 2011, p. 159.

institutos para abrigar a tutela integral do indivíduo. Esta compreensão foi reafirmada na própria justificativa da Proposta de Emenda Constitucional n. 19/2019, ao salientar a a autonomia do direito à proteção de dados em relação à privacidade.[17]

Neste sentido, ao se analisar, por exemplo, a proteção da intimidade e da vida privada (artigo 5º, inciso X, da Constituição da República), depreende-se que a ideia de privacidade é demasiadamente ampla, razão pela qual parte da doutrina vem defendendo a adoção de um "conceito plural", que possa se conectar com diversas situações que tangenciem a temática.[18] Contudo, ainda que se sustente uma visão ampla de privacidade, nem todos os aspectos dos dados pessoais guardam relação com aquele primeiro direito. Certas informações, como a divulgação do número da carteira de habilitação, não acarretariam risco direto à privacidade do indivíduo; porém, a forma como esse dado será tratado poderá acarretar outras espécies de violações.

Busca-se demonstrar, em síntese, que em decorrência de seu caráter individual e privado, o direito à privacidade não seria eficaz para resolver todas as lides envolvendo o tratamento de dados pessoais. A proteção autônoma deste último direito, por seu turno, possui dimensão coletiva e se caracteriza pela liberdade positiva[19] relacionada ao tráfego de informações e certo controle sobre essa circulação.

E o mesmo fenômeno pode ser sublinhado na relação com outros direitos fundamentais, como o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, insculpido no artigo 5º, inciso XII, da Constituição da República. A respeito, Laura Schertel Ferreira Mendes destaca a lição de Tercio Sampaio Ferraz Jr, incorporada pela jurisprudência do Supremo Tribunal Federal, para quem o dispositivo citado "assegura o sigilo da comunicação de dados, mas não dos dados entre si".[20] Destarte, evidencia-se que o inciso XII do artigo 5º também não seria suficiente, por si só, para garantir a proteção de dados pessoais.

Outrossim, a autonomia do direito fundamental à proteção de dados também era justificada pelo caráter de expansividade do rol de direitos fundamentais, que, "*a teor do art. 5º, §2º, da CF, não se limita aos direitos expressamente contemplados*

---

[17] De acordo com a justificativa apresentada ao Senado: "*de fato, a privacidade tem sido o ponto de partida de discussões e regulações dessa natureza, mas já se vislumbra, dadas as suas peculiaridades, uma autonomia valorativa em torno da proteção de dados pessoais, de maneira, inclusive, a merecer tornar-se um direito constitucionalmente assegurado.*" BRASIL, Senado Federal. Justificação à proposta de Emenda Constitucional n. 17/2019, proposta em 12.03.2019, de lavra do Senador Eduardo Gomes. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em 23.02.2022.

[18] Para maior aprofundamento sobre o tema, cf.: SOLOVE, D. "I've got nothing to hide' and other misunderstandings of privacy, *San Diego Law Review*, Vol. 44, pp. 745-772, 2007, GWU Law School Public Law Research Paper nº 289; LEONARDI, M. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.

[19] Bruno Bioni destaca que a liberdade se caracteriza pela dicotomia público-privado: quanto ao aspecto negativo, "*pela liberdade negativa de o indivíduo não sofrer interferência alheia*" e por ser "*um direito estático à espera de que o seu titular delimite quais fatos da vida deveriam ser excluídos do domínio público*". Em contrapartida, a liberdade positiva qualifica a proteção de dados pessoais, uma vez que "*a esfera privada não seria algo já posto à espera de uma violação, mas um espaço a ser construído a posteriori e dinamicamente mediante o controle das informações pessoais. Haveria, por isso, uma mudança qualitativa representada pela transposição do eixo antes focado no trinômio "pessoa-informação-sigilo" ao eixo agora composto por quatro elementos "pessoa-informação-circulação-controle"*". BIONI, B. R. *Proteção de dados pessoais:* a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020, p. 93/94.

[20] MENDES, L. S. F. *Privacidade, proteção de dados e defesa do consumidor*: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. Versão eletrônica do Kindle.

pelo constituinte, mas abarca outros direitos decorrentes do regime e dos princípios da Constituição, bem como constantes dos tratados internacionais (de direitos humanos) ratificados pelo Brasil".[21]

O cenário traçado antes da aprovação da Emenda Constitucional n. 115/2022, portanto, demonstrou a relevância e a utilidade do reconhecimento de um direito fundamental autônomo à proteção de dados no contexto da sociedade contemporânea, tendo em vista sua especificidade face a outros direitos, bem como a atribuição de características que majoram a efetividade da tutela do indivíduo. Assim, louvável a atuação do Poder Constituinte Derivado no sentido de positivar o direito fundamental autônomo à proteção de dados pessoais.

3. O uso de cadastros de dados pessoais pelo setor público no direito comparado. Como a experiência de outros países pode auxiliar a compreensão da problemática sob análise?

A eficiência de bancos de dados automatizados rapidamente foi captada pelos mais diversos países, de maneira que logo começaram a surgir iniciativas de unificação de variados cadastros do setor público, organizando informações outrora esparsas. Esse movimento político, no entanto, desde cedo suscitou importantes debates sociais e críticas de autores especializados, sendo possível observar, ao longo da História, o retroceder dos intentos de uma administração pública onisciente. Neste tópico, serão examinados alguns exemplos do direito comparado, o que contribuirá para a construção de uma visão mais crítica sobre a adoção de práticas semelhantes no Brasil.

Iniciando-se o exame pelos Estados Unidos da América, cumpre citar a lição de Danilo Doneda sobre a proposta de criação, em 1965, do "*National Data Center*", o qual agregaria diversos cadastros da administração federal, sob o argumento da eficiência administrativa. Porém, críticos apontaram para o desequilíbrio na relação Estado-administrado, eis que o governo teria em seu poder informações detalhadas dos cidadãos, em confronto com a cultura liberal americana. À época, diversas audiências públicas foram conduzidas pelo Congresso Americano para debater o tema, as quais levaram à conclusão de que a inexistência de salvaguardas suficientemente hábeis a assegurar a liberdade e a privacidade do cidadão não justificaria eventuais ganhos para a eficiência na execução de políticas públicas.[22]

As tentativas norte-americanas de unificação de cadastros, todavia, não cessaram. Ao contrário, ganharam força após os ataques terroristas de 11 de setembro de 2001. A respeito, Daniel Solove alude aos sistemas almejados e métodos clandestinos efetivamente utilizados pela "*National Security Administration*" (NSA). Neste sentido, o autor cita a criação do projeto "*Total Information Awareness*", conduzido pelo Departamento de Defesa, objetivando a unificação de informações, a fim de traçar perfis e analisar comportamentos suspeitos. Após divulgação do projeto pela mídia, a repercussão social negativa ensejou o seu arquivamento. Contudo, ao longo do tempo tornou-se público, por exemplo, que o governo autorizou o monitoramento, pela NSA, de ligações telefônicas sem respaldo em mandado judicial. Também foi divulgado que a NSA fazia uso de informações financeiras sigilosas sem maiores garantias aos cidadãos.[23]

No artigo intitulado "*I've got nothing to hide and other misunderstandings of privacy*", Daniel Solove aduz que o sopesamento entre privacidade e segurança realizado por grande parte da sociedade tem favorecido o segundo valor, haja vista

---

[21] SARLET. I. W. "Fundamentos constitucionais: o direito fundamental à proteção de dados", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021 , p. 27.

[22] DONEDA, D. C. M. *Da privacidade à proteção de dados pessoais*: fundamentos da lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2020, Versão eletrônica do Kindle.

23 SOLOVE, D. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, pp. 745-772, 2007, GWU Law School Public Law Research Paper nº 289, pp. 745-746.

que o fim buscado – combate ao terrorismo – justificaria os meios eleitos, em especial porque o cidadão que não vive nas raias da ilegalidade nada teria a temer. Embora o autor demonstre as falácias deste argumento, a aparente conivência de setores sociais demonstra a importância de novos debates públicos sobre o tema. Por ora, para não extrapolar os estreitos limites deste artigo, cumpre apenas mencionar que uma análise mais sofisticada da matéria leva à conclusão de que o acesso a perfis completos da população pode gerar desequilíbrios e as mais variadas violações, prejudicando o próprio desenvolvimento da sociedade como um todo.[24]

Alternando-se o olhar para o continente Europeu, cita-se, novamente, o autor Danilo Doneda, que destaca a importância das experiências francesa e alemã. Assim, na França, a implementação da interconexão de dados pelo *Systeme Automatisé pour les Fichiers Admínístratifs et le Répertoire des Individus* (SAFARI) foi inviabilizada pelo Primeiro-Ministro em 1974, em virtude da repercussão negativa e da insurgência social contra a unificação dos bancos de dados. Poucos anos após, em 1978, promulgou-se a lei de proteção de dados na França.[25]

A Alemanha também possui importante histórico quanto à regulamentação da proteção de dados pessoais. Como mencionado anteriormente, o primeiro marco normativo surgiu em um Estado Alemão em 1970, e ficou conhecido como a Lei de Proteção de Dados de Hesse. Em 1977, foi promulgada a lei federal de proteção de dados, conhecida como "*Bundesdatenchutzgesetz"*.[26]

Para além da atividade legislativa, o Tribunal Constitucional Alemão proferiu, na década de 1980, a paradigmática decisão versando sobre a autodeterminação informacional como um desdobramento do direito ao livre desenvolvimento da personalidade. O caso tratava da constitucionalidade da Lei de 1982 que previa as condições do censo a ser realizado no ano seguinte. Referida lei possibilitava o uso das informações colhidas durante o censo para fins diversos, como a "*comparação dos dados levantados com os registros públicos e também a transmissão de dados tornados anônimos a repartições públicas federais, estaduais e municipais para determinados fins de execução administrativa*".[27]

O Tribunal não reconheceu a inconstitucionalidade da coleta de dados para o censo, dada a relevância e proporcionalidade dessa atuação na definição de estratégias estatais, que reverteriam em benefícios sociais. Contudo, após afirmar que "não existem mais dados insignificantes", a Corte entendeu que a autorização de compartilhamento dos dados para finalidades diversas daquelas estritamente estatísticas e o tratamento de dados pessoais sem a observância à anonimização e a processos que garantissem maior transparência aos titulares configuraria violação ao direito geral de personalidade, no tocante ao aspecto da autodeterminação sobre a informação.[28]

Interessa salientar que a decisão já indicava a necessidade de respeito ao que hoje podemos identificar como princípios da finalidade, necessidade, adequação e transparência, como aspectos garantidores de um desdobramento da personalidade, qual seja, a autodeterminação informativa. Em linhas concretas, o Tribunal garantiu

---

[24] SOLOVE, D. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, pp. 745-772, 2007, GWU Law School Public Law Research Paper nº 289.
[25] DONEDA, D. C. M. *Da privacidade à proteção de dados pessoais*: fundamentos da lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2020, Versão Eletrônica do Kindle.
[26] DONEDA, D. C. M. *Da privacidade à proteção de dados pessoais*: fundamentos da lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2020, Versão Eletrônica do Kindle.
[27] SCHWABE, J. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevideo: Fundación Konrad-Adenauer, 2005, p. 234.
[28] SCHWABE, J. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig et al. Montevideo: Fundación Konrad-Adenauer, 2005, pp. 234-245.

ao cidadão alemão o direito de maior controle sobre o tráfego das informações que lhe digam respeito. A importância deste julgado é inconteste, sendo que Danilo Doneda nos ensina que:

> Entre as várias leituras que a sentença alemã permite, ela é representativa de uma tomada de posição pela concepção segundo a qual os dados pessoais merecem proteção, visto que são manifestações diretas da personalidade, e, portanto, que sua órbita de proteção pertence à órbita dos direitos fundamentais e que nesta configuração devem se confrontar os demais interesses envolvidos.[29]

De se ressaltar a visão autônoma desse direito aferido pelo Tribunal, que possibilita a maior conscientização sobre o tráfego de dados pessoais, permitindo a autodeterminação informacional, que, segundo a doutrina, pode ser conceituada como "*o direito de cada indivíduo poder controlar e determinar (ainda não de modo absoluto) o acesso e o uso de seus dados pessoais*".[30]

Ressalta-se que a autodeterminação informativa não se confunde com o conceito de consentimento, em especial quando se aborda, como neste artigo, a relação Estado-administrado, caracterizada pela assimetria. Na realidade, extrai-se do julgado que a autodeterminação informativa tem seus contornos também definidos pelos princípios da finalidade, adequação, necessidade, dentre outros.

A grande relevância da decisão em análise pode ser comprovada pelo fato de que diversos ordenamentos jurídicos passaram a reconhecer o direito a autodeterminação informacional. Dentre eles o brasileiro, uma vez que a Lei Geral de Proteção de Dados[31] o prevê, no artigo 2º, inciso II, como um dos fundamentos da "disciplina da proteção de dados pessoais". O cumprimento dessa norma claramente deve guiar qualquer modalidade de tratamento de dados, o compartilhamento, inclusive.

4. O arquétipo normativo brasileiro

Como demonstrado, o tratamento de dados pessoais assumiu um papel de destaque na sociedade contemporânea, a ponto de possibilitar o alvorecer de um novo direito. Cumpre examinar, nesta oportunidade, a dimensão objetiva deste direito fundamental, especificamente no tocante ao uso compartilhado de dados na esfera pública.[32]

Para tanto, imprescindível a detida análise da Lei Geral de Proteção de Dados (Lei n. 13.709/2018), cujo escopo protetivo abrange tanto o direito autônomo objeto

---

[29] DONEDA, D. C. M. *Da privacidade à proteção de dados pessoais*: fundamentos da lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2020, Versão eletrônica do Kindle.

[30] SARLET. I. W. "Fundamentos constitucionais: o direito fundamental à proteção de dados", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, p. 26.

[31] É importante registrar que a Lei Geral de Proteção de Dados Brasileira inspirou-se na GDPR (*General Data Protection Regulation*), norma promulgada pelo Parlamento Europeu e pelo Conselho da União Europeia, que estabelece regras relacionadas à proteção de dados dos países que integram o mencionado bloco econômico.

[32] Segundo Ingo Wolfgang Sarlet, a definição de um direito como fundamental veicula uma "*dupla dimensão – subjetiva e objetiva –, cumprindo uma multiplicidade de funções na ordem jurídico-constitucional*". Para o autor, o aspecto subjetivo está atrelado tanto a "*posições subjetivas de natureza defensiva (negativa)*", como ao direito a prestações positivas do Estado. Consequentemente, referido enfoque abarca a elaboração de normas jurídicas que prevejam desdobramentos do direito fundamental, como é o caso dos artigos 17 a 22 da Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Por seu turno, a dimensão objetiva relaciona-se à importância que as normas constitucionais sobre direitos fundamentais possuem como parâmetro para todo o ordenamento jurídico e a Administração Pública, incluindo a própria definição de procedimentos que assegurem a efetiva tutela do direito. (SARLET. I. W. "Fundamentos constitucionais: o direito fundamental à proteção de dados", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, pp. 41/47.

deste artigo[33], quanto os demais direitos interrelacionados, como, por exemplo, igualdade, liberdade, intimidade, vida privada e autodeterminação informativa.

Uma simples leitura da norma permite identificar que tais direitos são resguardados a partir das diretrizes e dos princípios listados, os quais configuram verdadeiro marco a ser observado no tratamento de dados pessoais realizado tanto pelo poder público, como pela iniciativa privada. Neste aspecto, cumpre ressaltar que, embora haja regulamentação de atividades públicas e privadas, o legislador reconhece as particularidades de cada setor, sendo que a Lei n. 13.709/2018 estabelece comandos normativos gerais e específicos para as diferentes espécies de agentes que venham a realizar o tratamento de dados pessoais.[34]

Assim, os dez princípios que regem as atividades de tratamento de dados, previstos no artigo 6º da Lei[35] em questão, consagram salvaguardas aos titulares, de modo que o poder público também se encontra vinculado à sua observância. Dentre eles, cumpre citar, em um primeiro momento, o da finalidade. Nos termos do texto legal, respeitará o princípio da finalidade o tratamento de dados "*para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades*". Por conseguinte, o dado pessoal deve ser tratado de acordo com determinado propósito, não se admitindo sua alteração, salvo nas circunstâncias legalmente autorizadas.

Merece destaque, igualmente, o princípio da adequação, que impõe a "*compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento*". Depreende-se que o dado pessoal colhido deve guardar pertinência com os fins almejados na atividade de tratamento. Para além da adequação, cabe ressaltar que o princípio da necessidade impõe que o tratamento recaia apenas sobre a quantidade mínima de dados que garanta o atingimento da finalidade almejada e previamente informada pelo agente, sendo vedados excessos injustificáveis.

Por derradeiro, ressalta-se que o princípio da transparência (artigo 6º, inciso VI) possui relevante destaque quanto à autodeterminação informacional, por

[33] Vide art. 5º, inciso LXXIX, da CF/88.

[34] Vide Capítulo IV da Lei 13.709/2018.

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

representar a garantia de que o titular poderá ter conhecimento sobre etapas do processo de tratamento de dados.[36]

O respeito ao rol legal de princípios deve ser acompanhado do respaldo em alguma das bases legais previstas nos artigos 7º e 10 ou, em caso de dado pessoal sensível, no artigo 11 da Lei n. 13.709/2018. Este diploma arrola diversos fundamentos, como consentimento, cumprimento de obrigação legal, execução de contrato, proteção do crédito, o legítimo interesse, dentre outros. Válido destacar que o consentimento não é exigido em toda e qualquer modalidade de tratamento de dados pessoais, tendo em vista que, em certas hipóteses, a obtenção da manifestação de vontade não se afiguraria viável. A Lei n. 13.709/2018, reconhecendo esta dificuldade, não eleva a base legal do consentimento a hierarquia superior às demais, exceto quanto ao tratamento de dados pessoais sensíveis, em razão de sua natureza.[37]

Diante deste cenário, tem-se que o poder público atuará, geralmente, amparado na base legal da execução de políticas públicas (artigos 7º, inciso III,[38] e

---

[36] Serão tecidas considerações mais aprofundadas sobre o princípio da transparência no tópico seguinte. Demais disto, a previsão legal acerca da transparência busca evitar o fenômeno que Daniel Solove descreve como a metáfora kafkaniana do livro "O Processo": "*Franz Kafka's The Trial, which depicts a bureaucracy with inscrutable purposes that uses people's information to make important decisions about them, yet denies the people the ability to participate in how their information is used.52 The problems captured by the Kafka metaphor are of a different sort than the problems caused by surveillance. They often do not result in inhibition or chilling. Instead, they are problems of information processing—the storage, use, or analysis of data—rather than information collection. They affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives"*. Tradução livre: "*O Julgamento de Franz Kafka retrata uma burocracia que utiliza informação das pessoas para tomar decisões importantes sobre elas, mas nega às pessoas a capacidade de participar do processo de decisão acerca do uso dessas informações. Os problemas capturados pela metáfora Kafka são de um tipo diferente dos problemas causados pela vigilância. Muitas vezes não resultam em inibição. Na realidade, são problemas de processamento de informações — o armazenamento, uso ou análise de dados — em vez de coleta de informações. Afetam as relações de poder entre as pessoas e as instituições do Estado moderno. Eles não só frustram o indivíduo criando um sentimento de desamparo e impotência, mas também afetam a estrutura social alterando o tipo de relações que as pessoas têm com as instituições que tomam decisões importantes sobre suas vidas."* SOLOVE, D. "I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, pp. 745-772, 2007, GWU Law School Public Law Research Paper nº 289, pp. 756-757.

[37] Referido critério hierárquico pode ser aferido do próprio texto legal:
Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[38] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei. Vide, também, nota 29.

artigo 11, inciso II). Excepcionalmente, poderá se valer de outras modalidades, como o consentimento ou o cumprimento de obrigação legal.[39] A respeito, quanto à possibilidade do uso de outras bases legais pelo Estado, Miriam Wimmer assevera que:

> Embora a Lei não traga respostas claras quanto a essa questão, é interessante notar que, na experiência europeia, tem-se entendido que o Estado deve atuar predominantemente com base em suas competências legais específicas, sendo explicitamente vedada, no GDPR, a possibilidade de processamento de dados pessoais por autoridades públicas, no desempenho de suas atribuições, com base na hipótese do legítimo interesse. Também o consentimento é uma hipótese normalmente tratada com desconfiança no contexto do tratamento de dados pessoais pelo Poder Público, dados o desbalanceamento na relação entre cidadão e Poder Público e a consequente dificuldade de se caracterizar tal consentimento como livre. Sob uma perspectiva pragmática, a possibilidade de revogação do consentimento a qualquer tempo representa outro grande inconveniente para seu uso como base legal para o tratamento de dados pessoais pelo Poder Público. A depender do caso, o embasamento de uma política pública estruturante no consentimento individual traria uma instabilidade incompatível com os objetivos buscados.[40]

Vislumbra-se, então, que as ponderações apresentadas configuram novas delimitações ao poder discricionário da Administração Pública com relação ao tratamento de dados pessoais, uma vez que deverá ser apresentada motivação suficiente que abranja tanto a escolha da base legal que ensejará a atividade, quanto a necessidade para a persecução do interesse público envolvido. Referido dever de motivar será ainda mais criterioso nas situações em que o uso do aparato da força estatal configurar uma desvantagem na relação jurídica com o administrado.

Não se pode olvidar, de outro turno, que o tratamento de dados pela Administração Pública, principalmente quando realizado sob a base legal da execução de políticas públicas, atrai a observância dos princípios e regras de Direito Administrativo, a exemplo da legalidade, eficiência etc. Destarte, impõe-se que a atividade em análise também seja norteada pelos princípios arrolados no artigo 37 da Constituição da República, nas Constituições estaduais e nas outras leis infraconstitucionais, como a Lei Federal n. 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

A esse respeito, Miriam Wimmer ressalta a importância da harmonização e concordância prática entre os princípios previstos na Lei n. 13.709/2018 e aqueles que regem a Administração Pública. Isso porque os princípios da supremacia do interesse público sobre o privado, da publicidade e da eficiência poderiam acentuar demasiadamente a assimetria entre Administração e administrado. Com efeito, o Estado detém informações detalhadas sobre os cidadãos, que, no entanto, nem

[39] Como mencionado por Miriam Wimmer, é o caso, por exemplo, de serviços prestados mediante anuência voluntária pelo cidadão ou dos dados de servidores públicos armazenados por departamentos de recursos humanos de instituições públicas. WIMMER, M. "O regime jurídico do tratamento de dados pessoais pelo poder público", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, pp. 280/281 e nota de rodapé n. 24)

[40] WIMMER, M. "O regime jurídico do tratamento de dados pessoais pelo poder público", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, p. 280.

sempre possuem a opção de não as fornecer, sob pena de serem alijados da prática de atos de cidadania e participação na sociedade.[41]

Referido controle, por certo, quando advindo do próprio Estado, gera incremento de riscos de violação de direitos. Não é por outro motivo que, conforme demonstrado no capítulo anterior, diversas leis de proteção de dados surgiram após a tentativa de criação de bases de dados unificadas.

5. Compartilhamento de dados no âmbito da administração pública

Diante de toda a sistemática apontada, denota-se que incumbe ao órgão ou pessoa jurídica de direito público, no exercício de deveres-poderes[42], respeitar o arcabouço normativo que abrange os princípios da Administração Pública, o direito fundamental à proteção de dados e as diretrizes delineadas na Lei n. 13.709/2018, no tocante ao uso compartilhado de dados[43], sob pena de violação dos direitos dos titulares.

De acordo com o artigo 7º, inciso III, da Lei n. 13.709/2018, admite-se o compartilhamento de "*dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres*". Quanto aos dados pessoais sensíveis, Miriam Wimmer destaca que o artigo 11, inciso II, alínea b, possui um escopo mais restrito, pois somente possibilita o uso compartilhado fundado em leis ou regulamentos, não fazendo referência às hipóteses amparadas nos demais instrumentos arrolados no artigo 7º.[44]

Depreende-se da leitura da norma que a própria definição da base legal relativa à execução de políticas públicas antevê a possibilidade do uso compartilhado de dados, o que constitui um aceno ao princípio constitucional da eficiência na Administração Pública.[45] Todavia, a eficiência não configura um valor isolado, devendo ser interpretada à luz das garantias do titular de dados, ressaltando-se aquelas decorrentes de um direito fundamental à autodeterminação informacional.

Por esta razão, a Lei n. 13.709/2018, em seus artigos 6º, inciso VI, e 9º, inciso V,[46] assegura ao indivíduo a transparência no processo de tratamento de dados,

---

[41] WIMMER, M. "O regime jurídico do tratamento de dados pessoais pelo poder público", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, pp. 278/279.

[42] Cf., a respeito, a visão de Celso Antônio Bandeira de Mello sobre o princípio da supremacia do interesse público sobre o privado, para quem "*as prerrogativas que nesta via exprimem tal supremacia não são manejáveis ao sabor da Administração, porquanto esta jamais dispõe de 'poderes', sic et simpliciter. Na verdade, o que nela se encontram são 'deveres-poderes' (...). Isso porque a atividade administrativa é desempenho de função. Tem-se função apenas quando alguém está assujeitado ao dever de buscar, no interesse de outrem, o atendimento de certa finalidade. (...) Logo, aquele que desempenha função tem, na realidade, deveres-poderes*". MELLO. C. A. B. *Curso de direito administrativo***.** 33ª ed., rev.e atual. até a Emenda Constitucional 92, de 12.7.2016. São Paulo: Malheiros, 2016, p. 100.

[43] Segundo o artigo 5º, inciso XVI, da Lei n. 13.709/2018, o uso compartilhado de dados consiste em: "*comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados*".

[44] WIMMER, M. "O regime jurídico do tratamento de dados pessoais pelo poder público**",** em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, p. 279.

[45] Miriam Wimmer tece semelhante observação ao comentar o artigo 25 da Lei, que prevê a manutenção de dados em formato interoperável e estruturado para o uso compartilhado. WIMMER, M. "O regime jurídico do tratamento de dados pessoais pelo poder público", em BIONI, B. R. (*et al.*) *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021, p. 282.

[46] Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre

abrangendo a obrigação de prestar os devidos esclarecimentos sobre compartilhamento e finalidade. O artigo 23, inciso I, [47] reforça esse ideal, ao determinar à Administração o dever de informar sobre a realização de tratamento de dados e a respectiva finalidade desta atividade.

Por derradeiro, o artigo 26, *caput*, da Lei n. 13.709/2019 condiciona o compartilhamento no setor público ao respeito "*das finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas*". Entende-se que o objetivo da norma é estreitar o campo do uso compartilhado, não admitindo a adoção de justificativa baseada na execução de uma política pública genérica, o que poderia abarcar qualquer situação na esfera pública. Também deverá ser demonstrada a pertinência do compartilhamento com o desempenho competencial das instituições públicas, não se admitindo o desvio de finalidade.

A Lei n. 13.7089/2018, portanto, estabelece como principais balizas ao uso compartilhado de dados pessoais pela Administração Pública os deveres de transparência perante os titulares e respeito à finalidade, à adequação e à necessidade. Tais considerações perpassam pela execução de uma política pública específica e pela consonância ao desempenho das competências legais do órgão público ou pessoa jurídica. Ademais, em um Estado Democrático Constitucional de Direito, o dever de prestar contas classifica-se como um imperativo constitucional,[48] além de também estar positivado na Lei Geral de Proteção de Dados.[49]

Passa-se, então, à análise do Decreto n. 10.046/2019, expedido no âmbito do poder normativo regulamentar, que, nos termos de sua ementa, "*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.*"

---

acesso: (...) V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;(...)

[47] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (...)

[48] Georges Abboud, neste ponto, ensina que "*a conquista do constitucionalismo referente à limitação de poderes, inclusive o da administração pública, além de ser consectária da consagração de direitos fundamentais, do dever de motivar e dos princípios da moralidade e impessoalidade, é também fruto da evolução do processo civilizatório das sociedades sob a égide do constitucionalismo*". Quanto ao ideal de "*accountability"* e democracia, esclarece o autor que "*na ideia de representação está presente a ideia de accountability (dever de prestar contas mediante critérios racionais e previamente estabelecidos). Ou seja, de algum modo o governante é considerado responsável pela forma como age em nome daqueles que o elegeram"*. ABBOUD, G. *Processo constitucional brasileiro*. 4ª ed. São Paulo: Thompsom Reuters Brasil, 2020. pp. 61 e 1.341. O autor defende, a nosso ver acertadamente, que o paralelo entre uma democracia forte e frágil advém do grau de implementação de mecanismos de prestação de contas, reforçando a ideia de que devemos exigir os mais diversos instrumentos de "*accountability"* no exercício dos deveres-poderes administrativos, de modo a conferir força aos imperativos constitucionais e ao compromisso democrático assumido em 1988.

[49] Cf. Art. 6º, inciso X, da Lei Geral de Proteção de Dados: "X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

De sua leitura, podem ser apreendidas certas violações ao arquétipo normativo acima delineado, em especial diante da clara prevalência da defesa do princípio da eficiência em detrimento dos direitos dos cidadãos. Neste sentido, destacam-se, de proêmio, os objetivos do compartilhamento de dados arrolados no artigo 1º do mencionado decreto, tais como a simplificação da oferta de serviços públicos; a otimização na implementação e no monitoramento de políticas públicas, bem como no acesso ou manutenção de benefícios sociais e fiscais; o zelo na custódia dos dados, com incremento da eficiência e qualidade na atuação da administração pública federal. Ou seja, o espírito da norma aparenta realizar uma ponderação prévia entre valores, presumindo a preponderância de uma gestão pública mais eficiente.

No mais, nos termos da primeira diretriz arrolada no artigo 3º do decreto, a "*informação do Estado será compartilhada da forma mais ampla possível*"[50]. A asserção, por si só, demonstra incompatibilidade com a Lei n. 13.709/2018, que prevê o compartilhamento de dados em situações específicas. O artigo 5º, por sua vez, dispensa a celebração de convênios ou outras modalidades de parcerias entre órgãos e entidades da Administração Pública federal e o artigo 8ª estipula ao custodiante de dados compulsoriedade no fornecimento a integrantes da estrutura pública a nível federal.[51]

Outrossim, há a criação de três níveis de compartilhamentos de dados, "de acordo com a sua confidencialidade": amplo, restrito e específico. Basicamente, a classificação dispõe que os dados não sigilosos não estarão "sujeitos a nenhuma restrição de acesso".[52] Ora, os níveis desconsideram toda a teoria na qual se funda a novel legislação de proteção de dados. Como visto, a proteção de dados é direito autônomo positivado na Constituição, e não se submete à dicotomia dado público e privado. Na realidade, todo dado relativo à pessoa natural, ainda que publicizado, merece algum nível de proteção, não havendo espaço, portanto, para compartilhamento amplo ou irrestrito, ou, ainda, compartilhamento restrito, porém, "simplificado" e a ser acessado por diversos órgãos e entidades.

Não se olvida o dever de atenção ao princípio constitucional da publicidade e o direito de acesso a informações governamentais, amparados pelo artigo 5º, inciso XXXIII, e artigo 37, §3º, inciso II, ambos da Constituição da República, bem como pela lógica da Lei n. 12.527/2011[53]. Contudo, a publicização de tais informações não se confunde com os dados pessoais, ainda que estes tenham se tornado públicos. E o Decreto n. 10.046/2019, ao prever os mecanismos supramencionados, não realiza

---

[50] Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes: I - a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais.

[51] Art. 8º Os custodiantes de dados disponibilizarão aos órgãos e às entidades de que trata o art. 1º os dados de compartilhamento amplo e restrito hospedados em suas infraestruturas tecnológicas, por meio das plataformas de interoperabilidade, condicionado à existência de solicitação de interoperabilidade e à ciência ao gestor dos dados.

[52] 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.

[53] Conhecida como Lei de Acesso à Informação, que "*regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências*."

qualquer distinção entre compartilhamento de dados pessoais e de informações sobre a Administração Pública, criando margem para o livre intercâmbio de dados pessoais entre variadas entidades que compõem a estrutura administrativa federal. Referida interpretação deverá ser combatida, sob pena de violação ao direito fundamental à proteção de dados pessoais.

Percebe-se que, apesar de o decreto fazer menção à Lei n. 13.709/2018, passa ao largo da necessidade de observância de princípios cruciais e fundantes da legislação, como os princípios da finalidade, adequação, necessidade, transparência e *accountability*[54]. Isso porque permite o compartilhamento de dados em demasia, independentemente do respeito à execução de políticas públicas específicas e que guardem relação com o mister institucional do ente da administração federal.

Constatam-se, ainda, violações das normas de Direito Administrativo. A dispensa geral de celebração de convênios ou instrumentos similares enfraquece princípios administrativos como o da motivação, uma vez que a adoção de qualquer ação pela Administração Pública deve estar pautada em fatos e fundamentos jurídicos que a sustentem.[55] Compreende-se que a ausência de convênios e demais instrumentos congêneres somente seria justificada na hipótese em que o compartilhamento se encontre fundamentado em leis ou regulamentos que resguardem a autodeterminação informativa, o que também não ocorre segundo a sistemática adotada pelo Decreto n. 10.046/201. A celebração de convênios e instrumentos similares ou a elaboração de normas específicas permitiria a verificação concreta de adoção por parte do Poder Público de boa procedimentalização e governança na atividade de tratamento de dados, além de observar o postulado da transparência e viabilizar a prestação de contas, o que é indispensável à atuação do Poder Público em regimes democráticos.

Além disso, o ato presidencial não prevê o dever de esclarecimento ao titular sobre o compartilhamento para finalidade diversa, ou, ainda, a necessidade de coleta apenas de dados indispensáveis e adequados para a persecução da finalidade eleita, afrontando a autodeterminação informacional, incorporada pelo ordenamento jurídico pátrio pela Lei Geral de Proteção de Dados.

Por fim, cumpre ressaltar que o art. 16 do mencionado decreto instituiu o Cadastro Base do Cidadão, que consiste em uma "*base integradora e pelos componentes de interoperabilidade necessários ao intercâmbio de dados dessa base com as bases temáticas, e servirá como base de referência de informações sobre cidadãos para os órgãos e entidades do Poder Executivo federal*." Referida base de dados centralizada foi implementada com objetivo de aprimorar a execução de políticas públicas e de "*facilitar o compartilhamento de dados cadastrais do cidadão entre os órgãos da administração pública*", além de permitir o "*cruzamento de informações das bases de dados cadastrais oficiais a partir do número de inscrição do cidadão no CPF*".

Evidencia-se a ausência de quaisquer salvaguardas minimamente satisfatórias aos direitos dos cidadãos na regulamentação desta base unificada de dados, não sendo possível aferir seus limites de modo claro e preciso. Com efeito, sequer há informação sobre quais órgãos federais ou órgãos da Administração Pública terão acesso à base de dados unificada do cidadão.

---

54 Tradução livre: responsabilidade. Esse princípio foi conceituado no artigo 6º, inciso X, da Lei Geral de Proteção de Dados (Lei 13.709/2018), *in verbis*: *X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas*.

55 Cf. Lei 9784/99, art. 50 Os atos administrativos deverão ser motivados, com indicação dos fatos e dos fundamentos jurídicos (...). § 1º A motivação deve ser explícita, clara e congruente, podendo consistir em declaração de concordância com fundamentos de anteriores pareceres, informações, decisões ou propostas, que, neste caso, serão parte integrante do ato.

Da leitura do dispositivo, extrai-se novamente a preferência conferida aos princípios da eficiência e supremacia do interesse público. Entretanto, são princípios que também devem ser observados pela Administração Pública a motivação, razoabilidade, proporcionalidade, incumbindo ao Poder Público sopesar a proteção aos direitos dos administrados com os fins colimados pela sua atuação, não havendo que se falar em prevalência, *prima facie*, de um princípio em detrimento do outro.

A regulamentação federal quanto à governança no compartilhamento de dados no âmbito da administração pública, portanto, revela pontos de flagrante incompatibilidade com a Constituição da República de 1988 e com a Lei Geral de Proteção de Dados. Denota-se que há contrariedade ao conteúdo do direito à proteção de dados, bem como que o decreto não se limita a regulamentar as leis que menciona para sua fiel execução, criando uma sistemática diversa da prevista na Lei n. 13.709/2018.

6. Conclusão

O paradigma atual determina que se contemple a integral proteção da pessoa face às evoluções tecnológicas e seus efeitos nas mais variadas esferas da vida social, a implicar mudanças na cultura jurídica. Neste aspecto, a recente incorporação da proteção de dados como direito fundamental autônomo e a edição da Lei n. 13.709/2018 instam o desenvolvimento de uma arquitetura jurídica composta de princípios e regras que assegurem a eficácia do referido direito e, em última medida, a dignidade da pessoa humana.

Como direito fundamental autônomo, a proteção de dados possui diversos pontos de conexão com outros direitos, mas com eles não se confunde. Como visto, por não se equiparar à privacidade ou ao direito ao sigilo, o direito ora sob exame abrange dados pessoais que não necessariamente exponham a intimidade do indivíduo. O olhar deve ser direcionado a outros aspectos, como o desequilíbrio nas relações jurídicas e a falta de transparência nos processos de tratamento de dados.

A coleta abusiva e o uso indiscriminado de informações pessoais prejudicam o livre desenvolvimento da personalidade dos indivíduos, principalmente, os menos favorecidos, que acabam sendo colocados à margem do processo tecnológico utilizado na datificação das relações, seja com o setor privado, seja com o público. Há, portanto, que se preservar o ser humano de ingerências indevidas no manejo de suas informações pessoais, bem como assegurar mecanismos de "*accountability*".

No presente artigo, buscou-se analisar um ponto específico do tratamento de dados pessoais, o qual envolve o compartilhamento de dados pessoais e a elaboração e execução de políticas públicas. Tentou-se demonstrar que, apesar de esta realidade ser indispensável para a persecução das finalidades estatais, tal atividade pode potencializar desequilíbrios na relação entre Estado e administrado.

A respeito, as experiências estrangeiras demonstram a necessidade de ponderação de interesses mediante análise de casos concretos, sendo que não devemos nos curvar a discursos que, embora sedutores, baseiam-se em premissas que não se sustentam quando alvo de um olhar mais cuidadoso. Em outras palavras, argumentações que priorizam a supremacia do interesse público sobre o privado ou eficiência administrativa, ainda que mediante sacrifício de outros direitos, não devem ser adotados *prima facie*.

No Brasil, o arquétipo veiculado pela Constituição da República de 1988 e pela Lei Geral de Proteção de Dados impõe a observância de diversos princípios e diretrizes, que devem ser interpretados de maneira harmônica, a fim de não restringir desproporcionalmente os direitos individuais. No entanto, diante do Decreto Presidencial n. 10.046/2019, verifica-se o não cumprimento destes objetivos, uma vez que possibilita o compartilhamento indiscriminado de dados entre diversos atores que compõem a administração pública federal.

Para que haja uma procedimentalização ideal, o compartilhamento deve ser motivado e pautado pelos princípios da finalidade, necessidade, adequação e transparência, respeitando-se, ademais, a autonomia informacional. Afinal, para o

bom funcionamento de uma democracia, a Administração Pública deve sempre reger suas ações na prestação de contas à sociedade (princípio de "*accountability*").

7. Referências

BARROSO, L. R. *Curso de direito constitucional contemporâneo:* os conceitos fundamentais e a construção do novo modelo. 3ª ed. São Paulo: Saraiva, 2011

BIONI, B. R. *Proteção de dados pessoais* - A função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020

BIONI, B. R. (*et al.*). *Tratado de proteção de dados pessoais*. 2ª reimp. Rio de Janeiro: Forense, 2021

DONEDA, D. C. M. *Da privacidade à proteção de dados pessoais:* elementos da formação da Lei Geral de Proteção de Dados. 2ª Ed. São Paulo: Thomson Reuters Brasil, 2020. Versão eletrônica do Kindle

EUBANKS, V. *Automating inequality.* New York: St. Martin's Publishing Group: 2018, Versão eletrônica do Kindle

LEONARDI, M. *Tutela e privacidade na internet.* São Paulo: Saraiva, 2012

MELLO, C. A. B. *Curso de direito administrativo.* 33ª ed., rev.e atual. até a Emenda Constitucional 92, de 12.7.2016. São Paulo: Malheiros, 2016

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

PASQUALE, F. *The black box society,* Cambrigde, Massachusetts, London, England: Harvard University Press, 2015. Versão eletrônica do Kindle.

SCHWABE, J. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.* Organização e introdução: MARTINS, L. Prefácio: WOISCHNIK, J. Trad. HENNIG, B. et al. Montevideo: Fundación Konrad-Adenauer, 2005

SOLOVE, D. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, pp. 745-772, 2007, GWU Law School Public Law Research Paper nº 289

WARREN, S.; BRANDEIS, L. "The right to privacy", Harvard Law Review, v. IV, n. 5, 1890 Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 19 set. 21