EXCELENTÍSSIMO SENHOR RELATOR MINISTRO GILMAR MENDES DO SUPREMO TRIBUNAL FEDERAL

Ação Direta de Inconstitucionalidade nº 6.649

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, já devidamente qualificado nos autos da presente Ação Direta de Inconstitucionalidade, vem, respeitosamente, perante Vossa Excelência, na qualidade de **AMICUS CURIAE,** apresentar intervenção, nos termos do artigo 138 do Novo CPC c/c o artigo 323 do RISTF, pelos fatos e fundamentos expostos a seguir.

I. SÍNTESE DOS FATOS E DOS PEDIDOS DA AÇÃO

O Conselho Federal da Ordem dos Advogados do Brasil (OAB) ajuizou, no Supremo Tribunal Federal (STF), a Ação Direta de Inconstitucionalidade (ADI) 6649, contra o Decreto 10.046/2019 da Presidência da República, 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. A ação foi distribuída, por prevenção, ao ministro Gilmar Mendes, relator da Arguição de Descumprimento de Preceito Fundamental (ADPF) 695, que questiona o mesmo decreto.

A petição inicial do Conselho Federal da Ordem dos Advogados do Brasil foi protocolada em 23/12/2020. A ação do CF/OAB tem como ato normativo pugnado o Decreto nº 10.046, de 09/10/2019, 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". A ação sustenta que o Decreto nº 10.046/2019 ostenta inconstitucionalidades formais e materiais. Primeiro, quanto às inconstitucionalidades formais, o decreto invade matérias de competência privativa de lei, exorbitando os poderes normativos concedidos pela Lei Fundamental ao Presidente da República, em afronta ao artigo 84, incisos IV e VI, 'a'". Segundo, "no tocante às inconstitucionalidades materiais, o ato infralegal viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa".

A ADI afirma que o Decreto nº 10.046/2019 "contraria a ordem constitucional", notadamente a recente decisão do Plenário do Supremo Tribunal Federal que ratificou a decisão cautelar deferida na Ação Direta de Inconstitucionalidade 6.387/DF - proposta pelo Conselho Federal da Ordem dos Advogados do Brasil - e nas ADIs 6.388/DF, 6.389/DF, 6.390/DF e 6.391/DF.

O Conselho Federal da OAB sustenta que sob o argumento de que as medidas previstas no Decreto nº 10.046/2019 facilitarão o acesso dos brasileiros a serviços públicos federais, "está sendo erigida uma ferramenta de vigilância estatal extremamente poderosa, que inclui informações pessoais, familiares e laborais básicas de todos os brasileiros, mas também dados pessoais sensíveis, como dados biométricos". A petição dá ênfase à possibilidade de análise de "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (art. 2º, II, do Decreto nº 10.046/2019).

Argumenta-se, ainda, que dentre as finalidades previstas no artigo 1º do Decreto nº. 10.046/2019, "nenhuma objetiva o tratamento adequado e transparente dos dados pessoais" e que,

como consequência, o Decreto do Cadastro Base do Cidadão está em “total desarmonia” com a Lei 13.709/2018, a Lei Geral de Proteção de Dados Pessoais.

A ação sustenta que não há condições para aferição e avaliação da adequação e necessidade do compartilhamento pelos órgãos do governo federal - entidades da administração pública direta federal e indireta -, incluindo não só o Poder Executivo Federal, como também os demais Poderes. Para a Ordem dos Advogados do Brasil, "o Decreto nº 10.046/2019 não possibilita uma análise do contexto do uso das informações, das hipóteses previstas para compartilhamento de dados, da finalidade de sua utilização, dos riscos a que ficam expostos os cidadãos e da legitimidade das atividades envolvendo tratamento de dados pessoais". Tem-se como tese que a LGPD não admite a integração a priori dos dados em um cadastro unificado e gigantesco. De acordo com a ação, "interligar bases de dados e permitir o seu cruzamento sem critérios devidamente esclarecidos enfraquece o direito à autodeterminação informativa".

A ação foi elaborada antes da instituição da Autoridade Nacional de Proteção de Dados Pessoais (ANPD), hoje em plena operação.[1] Na ação, argumenta-se que a não instalação da ANPD “fragiliza ainda mais os direitos fundamentais à privacidade e à proteção de dados pessoais”. Para os autores da ação, "a criação de um cadastro colossal unificado com um sistema de governança deturpado que apresenta evidente risco de violação de dados pessoais de todos os brasileiros, o ato normativo não resiste a uma verificação pautada pelo bom senso do razoável".

Em síntese, a Ordem dos Advogados do Brasil defende que o decreto restringe de forma indevida a privacidade e a proteção de dados para promover o acesso à informação e o compartilhamento de dados. Assim, pede-se a concessão de medida liminar monocraticamente pelo Ministro Relator, ad referendum do Plenário (art. 10, § 3º, da Lei 9.868/1999), para: i) suspender imediatamente a eficácia da integralidade do Decreto nº 10.046/2019 (e, consequentemente, do Decreto 10.403/2020, que alterou dispositivos do Decreto 10.046/2019), ad referendum do Plenário desse Pretório Excelso, e, ii) suspender imediatamente o Cadastro Base do Cidadão e para que cesse qualquer compartilhamento indevido de dados pessoais, sob pena de danos irreparáveis aos direitos fundamentais de toda a população brasileira, tornando inviável o retorno ao status quo ante. no mérito, pede a ação a a procedência da presente Ação Direta de Inconstitucionalidade, para declarar a inconstitucionalidade, na íntegra, do Decreto nº 10.046/2019 (e, consequentemente, do Decreto 10.403/2020, que alterou dispositivos do Decreto 10.046/2019), com a definitiva exclusão do Cadastro Base do Cidadão e do Comitê Central de Governança de Dados, na forma como foi concebido no decreto atacado.

[1] Ver https://www.gov.br/anpd/pt-br

Por meio da petição 453/2021 (eDoc 9), a Associação Data Privacy Brasil de Pesquisa requereu seu ingresso no feito, na condição de *amicus curiae*. Nos termos da decisão do Ministro Gilmar Mendes, em 07/01/2021, "tendo em vista a relevância da questão constitucional discutida e a representatividade da postulante, defiro, com fundamento no art. 6º, §1º, da Lei 9.882/1999, o pedido". Em 26/01/2021, foram deferidos os pedidos de ingresso do Laboratório de Políticas Públicas e Internet (Lapin) e do Instituto Mais Cidadania.

Apresentamos, a seguir, as contribuições na condição de *amicus curiae*, tendo em mente a complexidade da discussão em torno do Cadastro Base do Cidadão.

II. A CONTRIBUIÇÃO DO DATA PRIVACY BRASIL QUANTO AO OBJETO DA AÇÃO DIRETA DE INCONSTITUCIONALIDADE

Enquanto entidade civil sem fins lucrativos e dedicada à pesquisa em proteção de dados pessoais, nosso objetivo é, de um lado, reforçar a discussão em torno da natureza dos direitos à proteção de dados pessoais, e, de outro, contribuir com discussões que não foram suscitadas expressamente na petição do Conselho Federal da Ordem dos Advogados do Brasil, como a problemática em torno do conceito jurídico de uso compartilhado de dados e problemas relacionados ao princípio da minimização, previsto na Lei Geral de Proteção de Dados Pessoais, no desenho do Decreto 10.046/2019.

Inicialmente, trazemos uma discussão sobre o problema histórico da não concentração de dados pessoais em bases de natureza unificada, tendo como estudo de caso o *National Data Bank* nos Estados Unidos da América. Depois, discutimos a natureza da proteção de dados pessoais em sua dimensão procedimental e seus status constitucional como pontos de partida para a análise do Decreto 10.046/2019. Por fim, analisamos problemas específicos relacionados ao caráter potencialmente excessivo dos dados que podem ser acoplados à "base integradora" e a frouxidão dos mecanismos de verificação de interesse público no "uso compartilhado de dados". Apresentamos, por fim, uma proposta de teste de sopesamento para identificação do interesse público no uso compartilhado de dados, em oposição a uma ideia de *livre integração* ou *plena interoperabilidade de dados*.

A. Visão histórica de não concentração de poderes: o caso do *National Data Center*

A problemática trazida pelo Cadastro Base do Cidadão, em sua dimensão de uma interface de interoperabilidade unificada, remete, historicamente, aos debates em torno do *National Data Center*[2] nos EUA, uma das políticas públicas mais controversas com relação ao uso unificado de informações para fins de eficiência dos órgãos de planejamento do governo estadunidense.

No ano de 1965 o governo americano projetou uma estrutura capaz de reunir e armazenar diferentes informações sobre os cidadãos norte-americanos, tais como censo, registros trabalhistas, fiscais e de previdência. Existiam diversos argumentos favoráveis à proposta,[3] atrelados a uma lógica de eficiência: em regra, benefícios na gestão dos dados e eficiência dos órgãos em direta proporção ao volume de dados pessoais agregados. Em síntese, um banco centralizado como o National Data Bank[4] teria inegável potencial para produção de conhecimento e eficiência na administração pública.

A disponibilidade de dados poderia estimular pesquisas sobre problemas que, de outra forma, teriam a investigação difícil ou inviável, como é o caso da produção de etnografias em larga escala. Mais além, essa mesma disponibilidade possibilitaria usos genéricos dos dados - hoje, uma noção similar a usos futuros compatíveis com a finalidade consentida no tratamento inicial.[5] Dentre outras vantagens, estariam economia e eficiência na gestão do banco de dados; para fins científicos, amostras mais representativas e diversas, com maior grau de qualidade e permitindo generalização de resultados para toda a população; coleta de dados menos redundante, liberando mais tempo para a etapa de análise dos dados no lugar da coleta; melhor comparação entre variáveis, com mais facilidade de corrigir arbitrariedades; variáveis cobrindo mais áreas (como educação, economia, demografia, etc), propiciando combinações ricas e vantajosas para pesquisas; e análises mais fáceis

---

[2] DUNN JR, Edgar S. The idea of a national data center and the issue of personal privacy. **The American Statistician**, v. 21, n. 1, p. 21-27, 1967.

[3] Aqui, alguns elencados por Jack Sawyer e Howard Schechter em SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[4] Quanto ao nome adotado, Kaysen, membro de comitê específico para criação do NDB, indicou a preferência pela nomenclatura de National Data Bank no lugar de Federal Data Bank, o que possibilitaria a inclusão de dados estaduais e locais, mesmo que a proposta inicial fosse de dados apenas do governo federal. Estudos da época indicam que as propostas dos órgãos favoráveis à criação do NDB não deram atenção suficiente à privacidade, sendo que a maior preocupação do Congresso foi a proteção de dados pessoais. Nas sessões do Congresso, as propostas foram orientadas por prováveis usuários, incluindo universidades, entidades do meio privado, experts em computação e advogados de direito constitucional preocupados com liberdades civis. Ver: SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[5] CIPL. **Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR**. 19 maio 2017. p. 13. Disponível em: http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf. Acesso em: 02 fev. 2021.

de serem verificadas em termos de replicação,[6] trazendo maior rigor científico e superando empecilhos vivenciados principalmente por ciências sociais.[7]

Por outro lado, em que pese o entusiasmo de contribuições significativas, não foram poucas as críticas ao National Data Center. A atratividade da ideia não foi suficiente para eclipsar os riscos inerentes à formação de um banco de dados centralizado, como os altos custos em termos de privacidade individual e organizacional e segurança da informação.[8] À época, críticos da proposta deixavam claro que não eram alheios às possíveis contribuições do National Data Center nem o avaliavam como inerentemente negativo, mas sim traziam um olhar pragmático para implicações práticas e assim demonstraram que os riscos de um banco centralizado de dados eram tantos e tão variados que inviabilizavam a ideia em uma sociedade aberta e livre.

Das críticas apresentadas ao National Data Bank na década de 1960, não apenas muitas mantêm-se atuais, como também foram até mesmo agravadas. Já de início, a finalidade estatística foi debilitada pela constatação de que, a fim de obter as vantagens dos registros integrados, cada anotação deveria ser identificada individualmente. Um primeiro olhar sugeriria que dados agrupados seriam suficientes para análises mas, na prática, o cruzamento de variáveis diferentes (econômicas, sociais) - um dos grandes valores de um banco centralizado - *dependeria da individualização dos registros*. Em teoria, sempre haveria a possibilidade de extrair dados individuais de um banco centralizado, mesmo para arquivos classificados.[9]

O debate ocorrido na época é extremamente interessante. Constatou-se que a privacidade individual também enfrenta ameaças diretas pelo desenvolvimento da capacidade computacional de sistemas:[10] quanto maior a eficiência na coleta de dados, menos relevante é restringir a quantidade

---

[6] KING, Gary. Replication, replication. **PS: Political Science and Politics**, v. 28, n. 3, p. 444-452, 1995.

[7] Além desses, Hoffman identifica dentre os argumentos levantados por defensores da proposta: melhoria de registros históricos, muitas vezes perdidos; padrões e procedimentos para manutenção e documentação; possibilitar análise estatísticas de dados produzidos por órgãos e entidades que não têm esse preparo; facilidade e conveniência em registros, com ênfase em registros criminais e de inteligência; disponibilidade de dados para usos comerciais e do governo. Assim como Sawyer e Schechter, Hoffman identifica argumentos favoráveis à centralização de modo a situar o debate, logo em seguida apresentando críticas que colocam em xeque a compatibilidade entre um banco centralizado de dados pessoais com a tutela do direito à privacidade. Ver: HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[8] LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970.

[9] Por exemplo, mesmo que não haja interesse científico em investigar a resposta de um único indivíduo, computar as correlações no total, como renda e educação, exige a combinação entre a renda e os anos de estudo de cada pessoa em específico. Esse e outros pontos sobre a individualização de registros na prática são mais aprofundados em SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[10] LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970.

de dados coletados,[11] e os incentivos para restringir a coleta de dados pessoais ao mínimo necessário tornam-se menos atrativos;[12] com a redução de custos de armazenamento, o descarte de dados que seriam eliminados perde o senso de urgência; a facilidade de compartilhamento dos dados[13] torna o ato suscetível à banalização.

Além disso, de fácil inferência é o reconhecimento de que a tentação para acesso a tamanho volume de dados é alta, minimizada quanto maior seja o seu controle e o "preço" dessas informações sensíveis,[14] mas ainda inevitável. Ainda sobre o valor das informações pessoais centralizadas, ressaltou-se o risco de uso inapropriado dos dados, seja por entidades públicas ou privadas,[15] incluindo a relativização sobre finalidades de pesquisa[16] - o que, por consequência, veio acompanhado da ênfase em definições claras sobre o que deveria ser mantido, por quanto tempo e fortalecimento da legislação sobre privacidade e proteção de dados de modo geral.

O National Data Bank também foi criticado porque o argumento de autoridade da fonte e os danos à performance do sistema por inconsistência nos dados são riscos da proposta que, inclusive,

---

[11] "Since much more information on a person will be stored in the same place, less effort will be necessary to acquire certain 'sensitive' data." HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[12] E, por consequência, mais provável é a coleta de dados sem fins imediatos ou prospectivos em específico. Além disso, no processamento em larga escala, a manutenção de um dado pode ter custo menor do que seu descarte. LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970; HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[13] O que já preocupava à época é reforçado pelo desenvolvimento tecnológico: "it is now possible to disseminate materials quickly to widely scattered groups of interested recipients"; "National systems for the exchange of data, linking thousands of remote terminals, will shortly become commonplace. As they do, information that might formerly have been seen only by local custodians will be made readily available to agencies across the country". LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970.

[14] Além disso, mesmo nos casos em que não há erros, cumpre ressaltar que ainda subsistem problemas. Dados como entrevistas, avaliações pessoais e observações do tipo são altamente subjetivos e dificilmente verificáveis, o que ressalta a necessidade de um olhar crítico. Ver: HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969; SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[15] Riscos aumentados no caso de mau uso por entidades privadas ou públicas estaduais ou municipais, como em registros médicos, escolares e indústrias. HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[16] No debate, Scawyer e Schechter citam a Agência de Ciência e Tecnologia da Diretoria Executiva dos EUA, lembrando que a mesma centralização que ajuda o conhecimento (pesquisas em ciências sociais, por exemplo) ameaça à privacidade. conforme a Agência, a centralização ameaça dois principais valores na privacidade, sendo eles 1 - "privilege of making one's own decisions as to the extent to which one will reveal thoughts, feeling, and actions" e 2 - "the right to know anything that may be known or discovered about any part of the universe". Ainda comentando pesquisas envolvendo dados pessoais, os autores reconhecem o conflito entre a privacidade do indivíduo e o direito da sociedade ao conhecimento. Quanto ao ponto, apontou a literatura que o processamento de dados nos termos da proposta do National Data Center só se justificaria para fins com grande relevância social e desde que tomadas rigorosas medidas para promover a privacidade individual. Ver: SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

se retroalimentam. Isso porque o fato de uma fonte de dados ser considerada “oficial” desperta no imaginário popular um senso de confiabilidade que subestima as chances de erros e a necessidade de verificação.[17] Também não se ignora que a inconsistência dos dados pode trazer danos agravados à proporção da performance e eficiência de sistemas bem desenvolvidos.[18]

Por sua vez, a capacidade de armazenamento de dados interfere no senso de cronologia, fazendo com que os obsoletos tenham aparência e disponibilidade de dados recentes, ameaçando assim o direito ao esquecimento e mesmo segundas chances.[19] Tanto o resgate de informações antigas quanto o cruzamento de dados podem perpetuar e aprofundar intolerâncias:[20] qualquer mínimo desvio de conduta, desaprovado seja por teor ilícito ou não, coloca o indivíduo sob intenso escrutínio de autoridades e mesmo da coletividade. O caráter político do risco, que abre margem para vigilância massiva,[21] apresenta também implicações sociais como o aumento da intolerância e a restrição da diversidade.

Na mesma linha, o risco do perfilamento[22] não passou despercebido. Com o registro de informações sensíveis de forma centralizada, resta a possibilidade de “avaliação de cidadania”,[23] bem como outras formas de rotular indivíduos.

---

[17] “Systems with insufficient input checking might be given false and slanderous data about a person which, when printed out on computer output sheets as the result of an mqmry, looks quite "official" and hence is taken as true.” HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[18] “Furthermore, without public trust, information systems could well be fed so much false, misleading or incomplete information as to make them useless. Thus it becomes imperative not only to devise proper safeguards to data privacy, but also to convince the public and agencies which might contribute to a system that these safeguards are indeed being planned, and that they will work.” HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[19] SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[20] “These characteristics of large-scale personal information systems suggest quite significant new dangers for individual privacy. As an immediate matter, they lengthen and deepen institutional memories, thus reducing still further the likelihood that even isolated misconduct will be forgiven or forgotten”. LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970.

[21] "These systems threaten the creation of a society in which unorthodoxy is discouraged by its notoriety, and even the mildest eccentricities are catalogued for official evaluation."; “A society in which all of the data collected by government about an individual citizen were readily and permanently available for inspection would be one in which the opportunities for his supervision would be markedly increased.” LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n. 3, p. 207-211, 1970.

[22] “The same information that provides statistical analysis of overall manpower resources can serve to evaluate the individual for personal purposes”. SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[23] "A national data center has the potential to become a life history file employable by the Government to determine ‘worthiness’ to receive its resources. It could serve to decide if we were deserving of a job, a license, housing, a passport, welfare benefits, etc." SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

Além disso, já se atentava para a probabilidade de que as pessoas fornecessem seus dados em troca da conveniência dos serviços oferecidos,[24] de forma pouco crítica. Décadas depois, segue sendo o caso que, em que pesem desenvolvimentos jurídicos, a privacidade ainda é um conceito pouco compreendido pela população,[25] o que traz dificuldades em termos de consentimento informado sobre os dados coletados com essa base legal.

Ainda que não exaustivas, há uma série de medidas que se mostram imprescindíveis para uma proposta de centralização. Elas não eliminam os riscos inerentes à centralização, muito menos são capazes, por si só, de deixar a proposta mais plausível - consistem, ao contrário, em elementos mínimos a serem rigorosamente observados antes[26] de qualquer concretização. Controle de acesso,[27] monitoramento de ameaças, restrições em processamentos, gerenciamento de integridade (software, hardware e pessoas)[28] são alguns dos exemplos de soluções técnicas desejáveis[29] mas que,

---

[24] "We can expect a great deal of information about social, personal, and economic characteristics to be supplied voluntarily--often eagerly--in order to enjoy the benefits of the economy and the government". HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[25] A compreensão da privacidade é abordada na literatura enquanto *privacy literacy*, que pode ser definida como "the understanding that consumers have of the information landscape with which they interact and their responsibilities within that landscape". Não raro, o ponto é abordado junto ao conceito de alfabetização digital - para a American Library Association's Digital Literacy Task Force, "the ability to use information and communication technologies to find, evaluate, create, and communicate information, requiring both cognitive and technical skills". No Brasil, 74% dos brasileiros fornecem dados pessoais na hora de baixar apps. Ver: LANGENDERFER, Jeff; MIYAZAKI, Anthony D. Privacy in the information economy. **Journal of Consumer Affairs**, v. 43, n. 3, p. 380-388, 2009, p. 383; VISSER, Marijke. Digital Literacy and public policy through the library lens. **Maine Policy Review**, v. 22, n. 1, p. 104-113, 2013; KLEINA, Nilton. 74% dos brasileiros fornecem dados pessoais na hora de baixar apps. **Tecmundo**, 20 fev. 2015. Disponível em: https://www.tecmundo.com.br/apps/75271-74-brasileiros-fornecem-dados-pessoais-hora-baixar-apps.htm. Acesso em: 02 fev. 2021.

[26] SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968.

[27] Lembra Hoffman que é preciso proteger os dados para além do nível do arquivo, cuidando também do controle de acesso. Além disso, frisa o autor que tais medidas devem ser eficientes e não devem penalizar o indivíduo que opta por proteger apenas parte de seus dados. HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

[28] Atentando também para a necessidade de pensar códigos de ética profissional para a indústria tecnológica e para os que operam os dados, o que foi pontuado na discussão do National Data Center e segue ainda mais discutido atualmente. Quanto ao ponto, a interdisciplinaridade revela-se necessária também porque a capacitação dos profissionais de áreas técnicas em temas de privacidade e ética são mais sugeridas no meio acadêmico quando a composição dos autores envolve pessoas da área de humanas. Ver: HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969; SAWYER, Jack; SCHECHTER, Howard. Computers, privacy, and the national data center: The responsibility of social scientists. **American Psychologist**, v. 23, n. 11, p. 810, 1968; FAIRFIELD, Joshua; SHTEIN, Hannah. Big data, big problems: Emerging issues in the ethics of data science and journalism. **Journal of Mass Media Ethics**, v. 29, n. 1, p. 38-51, 2014; METCALF, Jacob; CRAWFORD, Kate. Where are human subjects in big data research? The emerging ethics divide. **Big Data & Society**, v. 3, n. 1, p. 1-14, 2016; O'LEARY, Daniel E. Ethics for big data and analytics. **IEEE Intelligent Systems**, v. 31, n. 4, p. 81-84, 2016.

[29] HOFFMAN, Lance J. Computers and privacy: A survey. **ACM Computing Surveys (CSUR)**, v. 1, n. 2, p. 85-103, 1969.

novamente, não afastam de forma satisfatória os altos riscos de um cenário de centralização de dados.[30]

B. O abandono do National Data Bank após o debate no Congresso dos EUA e o surgimento dos *Fair Information Practices Principles*

Em julho de 1966, o Comitê Gallagher organizou a audiência pública "The Computer and Invasion of Privacy"[31]. O relator chamou o projeto de "monstro", além de caro e pouco útil. Mais importante, Gallagher fez uma defesa vigorosa da precaução e de análise sobre potenciais violações de liberdades civis antes da implantação do National Data Bank, cujo orçamento já havia sido incluído na proposta orçamentária federal de 1967. O deputado republicano Frank Norton, membro do subcomitê, argumentou que a "privacidade é uma liberdade fundamental" e um "inquestionável direito constitucional", sendo que o problema da centralização de bases de dados e expansão dos computadores seria "semelhante às mudanças provocadas à vida nacional com a chegada da era nuclear" (House of Representatives, 1966, p. 5).

Em suas palavras, tal como dito na abertura da audiência pública de 26 de julho de 1966: "Não queremos nos privar das recompensas da ciência; queremos apenas garantir que a dignidade humana e as liberdades civis permaneçam intactas. Gostaríamos de saber quais informações seriam armazenadas em um data center nacional; quem teria acesso a ele; quem controlaria os computadores; e, o mais importante, como a confidencialidade e a privacidade individual seriam protegidas. Devemos pensar nessas questões agora, antes de acordarmos em alguma manhã no futuro e descobrirmos que o banco de dossiês é um fato estabelecido e que a liberdade como a conhecíamos desapareceu da noite para o dia" (House of Representatives, 1966, p. 5).

As audiências públicas no Congresso, somadas às intensas críticas feitas pela mídia e por acadêmicos (em especial Alan F. Westin e Arthur Miller) fizeram com que o governo desacelerasse a proposta, a fim de realizar estudos em profundidade sobre seus riscos. Um dos desdobramentos diretos foi a organização de um comitê sobre privacidade na American Federation of Information Processing Societies (AFIPS) e uma convenção nacional em abril de 1967. Outro desdobramento foi a

---

[30] Mesmo porque a extensão dos danos e sua reversibilidade são pontos tão mais críticos quanto maior seja a agregação dos dados. Exemplo recente nesse sentido é o vazamento de dados pessoais sensíveis de mais de 220 milhões de brasileiros divulgado no início de 2021, ainda em processo de investigação e já considerado um dos mais graves da história do país. Ver: G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. **G1**, 28 jan. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 02 fev. 2021.

[31] Ver as transcrições originais da audiência em https://archive.org/details/U.S.House1966TheComputerAndInvasionOfPrivacy. Acesso em 03 mar. 2021.

força tarefa presidencial sobre Armazenamento e Acesso de Estatísticas Governamentais, o chamado Comitê Kaysen.

A ascensão e declínio do National Data Bank serviram como oportunidade para uma espécie de "enquadramento" do debate sobre privacidade e proteção de dados pessoais nos EUA, dando origem a uma série de iniciativas legislativas que se iniciaram em 1969 e prosseguiram na década de 1970. O episódio do National Data Center é considerado pivotal para a primeira geração de legislações sobre proteção de dados pessoais.[32] Danilo Doneda explica que: "O debate sobre o National Data Center teve uma considerável ressonância na sociedade norte-americana e foi o incentivo a partir do qual iniciativas tomaram forma, como a formulação do Fair Credit Reporting Act (FCRA), a legislação sobre informes de crédito e dados pessoais, em 1970, ou mesmo o Privacy Act de 1974"[33].

Como sustentam Daniel Solove e Paul Schwartz, seguindo a tradição estadunidense de imposição de limites à atuação governamental, surgiu na década de 1960 um vigoroso debate sobre a determinação de direitos claros que pudessem superar a teoria de "invasão da propriedade"[34], definindo os limites de atuação do governo na execução de políticas públicas.[35] Esse debate ganhou novas dimensões com trabalhos como *Privacy and Freedom* (1967), de Alan Westin, que se dedicou à compreensão da privacidade como capacidade dos cidadãos de controlar os fluxos de dados gerados.[36]

Como sustenta Priscilla Regan, em 1965 "um novo problema foi colocado na agenda do Congresso e de subcomitês da Câmara [House] e do Senado [Senate]. O problema foi definido como a invasão da privacidade pelos computadores e evocava imagens de 1984 [livro de George Orwell], do Homem Computadorizado, e de uma sociedade do dossiê"[37]. Durante trinta dias foram realizadas audiências públicas sobre o tema. Essa discussão na esfera pública motivou a elaboração de um influente relatório pelo United States Department of Health, Education and Welfare (HEW) em 1972, durante a gestão Richard Nixon, que atacou o problema da privacidade e da coleta abusiva de dados pessoais por meio da proposição de uma base principiológica (*Code of Fair Information Practices*) estruturada em cinco pilares:

---

[32] SCHERTEL MENDES, Laura. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**, Revista dos Tribunais, 2019. p. 38.

[33] DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. In: MENDES, Laura Schertel et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 40.

[34] BIONI, Bruno; ZANATTA, Rafael. Direito e economia política dos dados: um guia introdutório. In: DOWBOR, Ladislau. (Org.). **Sociedade vigiada**. São Paulo: Autonomia Literária, 2020. p. 129.

[35] SOLOVE, Daniel; SCHWARTZ, Paul. **Information Privacy Law.** Sixth edition. New York: Wolters Kluwer, 2018. p. 36.

[36] WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.

[37] REGAN, Priscilla. **Legislating Privacy: technology, social values and public policy**. The University of North Carolina Press, 1995. p. 82.

a) Não deve haver sistemas de registro de dados pessoais cuja própria existência seja secreta;

b) Deve haver uma maneira de uma pessoa descobrir quais informações sobre ela estão em registro e como essa informação é usada;

c) Deve haver uma maneira de uma pessoa impedir que informações sobre ela, obtidas para um propósito específico, sejam usadas ou disponibilizadas para outros fins sem o consentimento da pessoa;

d) Deve haver uma maneira de uma pessoa corrigir ou ajustar um registro de informações identificáveis sobre a pessoa;

e) Qualquer organização que crie, mantenha, utilize, ou divulgue registros de dados pessoais identificáveis deve garantir a confiabilidade dos dados para o uso pretendido e deve tomar precauções para evitar usos indevidos dos dados;[38]

Esses cinco pilares formaram o eixo central dos *Fair Information Practices Principles* (FIPPs), que, na opinião de acadêmicos renomados como Marc Rotenberg (fundador da Electronic Privacy Information Center), se tornaram a principal moldura jurídica para estruturação das leis de proteção de dados pessoais nos EUA. Além disso, tornaram-se parâmetros para balizar a atuação do poder público, estimulando a identificação clara de **um propósito específico, em especial nos casos de usos secundários de uma informação ou conjunto de dados pessoais**.

Esses princípios influenciaram diferentes conjuntos principiológicos, como as *Fair Information Practices Principles* de São Diego e as *Privacy Guidelines* da OCDE, hoje amplamente conhecidas. O quadro abaixo apresenta os princípios em sua formulação original em língua inglesa:

Quadro 1. Comparação entre princípios de justiça para uso de dados (pelo poder público) e usos secundários de dados

Fair Information Practices U.S. Dept. of Health, Education and Welfare, 1973	***City of San Diego Fair Information Principles Adopted by San Diego City Council, October 1994***	***Privacy Guidelines Organization of Economic Cooperation and Development, 2013***
1. Collection limitation. There must be no personal data record keeping systems whose very existence is secret. 2. Disclosure. There must be a way for an individual to find out	1. Consideration of privacy effects. Privacy is recognized explicitly as an issue to be considered by the City in introducing and using information technologies.	1. Collection Limitation.There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge

[38] BIONI, Bruno; ZANATTA, Rafael. Direito e economia política dos dados: um guia introdutório. In: DOWBOR, Ladislau. (Org.). **Sociedade vigiada**. São Paulo: Autonomia Literária, 2020. p. 130.

what information about him is in a record and how it is used. 3. Secondary usage. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. 4. Record correction. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.	2. Openness. Citizens of San Diego have a right to know what personal information is collected about them by local government entities and how it is used. There must be no personal record-keeping system whose existence is secret. 3. Collection limitation. Only the personal information necessary for the stated purpose of the agency shall be collected. Whenever possible, such personal information shall be collected directly from the subject of the information. 4. Information integrity. Each local government agency shall make every reasonable effort to ensure that all records containing personal information are accurate and up-to-date and that procedures are in place to dispose of records once they are of no further use. 5. Access and correction. Citizens shall have reasonable means to obtain and review, and when necessary, correct and amend information about themselves held by local government entities. 6. Secondary usage. Personal information will not be made available for secondary uses without providing notice to the subjects of the information and allowing said subjects the means to opt out of such uses. However, consent is not required for secondary uses of personal information to support legitimate government activities such as law enforcement investigations, or for uses that are compatible with the purposes for which the information was first collected. 7. Security. The City will establish reasonable physical, technical and administrative safeguards to protect personal information against the risk of unauthorized access, collection, use, disclosure or disposal. 8. Education. The City will make reasonable efforts to educate San Diegans about the existence and	or consent of the data subject. 2. Data quality principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. 3. Purpose specification. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose. 4. Use limitation principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: (a) with the consent of the data subject; or (b) by the authority of law. 5. Security safeguards principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. 6. Openness principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller. 7. Individual participation principle. An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him,

	use of the broadband network for government services; its education efforts shall include how personal information is obtained, transmitted, used and stored by the City, and citizens' rights as expressed in these privacy principles. 9. Oversight. A mechanism for oversight and enforcement shall be established to ensure the observance of these principles. 10. Review. As information technologies advance, privacy considerations are likely to change. The City will review these principles on a regular basis to ensure their adequacy.	data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended. 8. Accountability principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Como será explicado a seguir, o Cadastro Base do Cidadão, ao ser composto pela **base integradora** e pelos componentes de interoperabilidade necessários ao intercâmbio de dados dessa base com as bases temáticas, servindo como **base de referência de informações sobre cidadãos** para os órgãos e entidades do Poder Executivo federal (art. 17, Decreto 10.406/2019), falha em promover um teste de compatibilidade que possa atestar a legitimidade do uso compartilhado dos dados originalmente coletados e utilizados para determinadas políticas públicas.

O problema jurídico do Cadastro Base do Cidadão está menos relacionado ao **cadastro em si (ou a ideia de interoperabilidade e uma base de referência sobre cidadãos)**, e muito mais sobre a ausência de um conjunto de salvaguardas que possa legitimar usos secundários de dados a partir de uma lógica de interface de interoperabilidade.

Antes de analisarmos o problema da ausência dessas salvaguardas, que terminam por macular determinadas partes do Decreto 10.046/2019, como o Capítulo III (“Das Regras Gerais de Compartilhamento de Dados”), apresentaremos os contornos do direito à proteção de dados pessoais em sua dimensão procedimental, tal como concebido pelo Supremo Tribunal Federal.

C. A natureza procedimental da proteção de dados pessoais e o reconhecimento do seu caráter autônomo

Em 06 e 07 de maio de 2020, esta Suprema Corte proferiu julgamento histórico, de ampla repercussão, sobre o direito à privacidade e à proteção de dados pessoais[39]. O objeto da análise da Corte nas ADIs 6387, 6388, 6389, 6390 e 6393 foi a Medida Provisória nº 954/2020[40], que estipulava o compartilhamento obrigatório de dados pessoais (nome, telefone e endereço) de empresas de telefonia móvel e fixa com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de continuidade da produção estatística do órgão.

Elementos como finalidade genérica, falha em precisar a necessidade do compartilhamento massivo de dados pessoais e ausência de medidas de segurança da informação motivaram o questionamento da constitucionalidade da medida[41] e, na ocasião, o Supremo Tribunal Federal decidiu por suspender a sua eficácia e impedir que a transferência dos dados se efetivasse.

O voto da ministra relatora Rosa Weber partiu de um pressuposto relacionado à natureza contextual dos dados pessoais. Hoje em dia, eles não mais se referem apenas a informações circunscritas à esfera íntima, privada, mas dizem respeito a quaisquer dados que possam, eventualmente, identificar um indivíduo. Nesse sentido, não há dados irrelevantes e, de acordo com o voto do ministro Luiz Fux, a concentração excessiva de informações, até as mais ''triviais'' (como o nome), carrega um potencial de violação aos direitos fundamentais dos indivíduos. Se esse potencial não era percebido há décadas, hoje, dado o estado do desenvolvimento tecnológico pautado no tratamento intensivo de dados pessoais, ele não pode mais ser ignorado[42].

Considerado o conjunto dos votos, o julgamento pautou-se em três aspectos principais, que podem ser extraídos como uma valiosa lição para a proteção de dados no Brasil: i) o direito à proteção de dados, embora não prescrito expressamente na Constituição, *é um direito fundamental*

---

[39] BRASIL. Supremo Tribunal Federal. **ADI 6387 MC-Ref / DF**. Relatora: Min. Rosa Weber. Órgão julgador: Plenário. Data de julgamento: 07/05/2020. Data de publicação: 12/11/2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 25 mar. 2021.

[40] BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 25 mar. 2021.

[41] Além da ADI 6387, ajuizada pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB), também foram apresentadas outras quatro ações, pelos seguintes partidos políticos: Partido Comunista do Brasil (PCdoB), Partido Socialismo e Liberdade (PSOL), Partido da Social Democracia Brasileira (PSDB) e Partido Socialista Brasileiro (PSB).

[42] THOMPSON, Stuart A.; WARZEL, Charlie. Twelve Million Phones, One Dataset, Zero Privacy. **The New York Times**, One nation, tracked: an investigation into the smartphone tracking industry, 19 dez. 2019. Disponível em: https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html. Acesso em: 11 mar. 2021.

autônomo, distinto do direito à privacidade (embora relacionado a ele); ii) o direito à proteção de dados é *um pilar da democracia em sua dimensão coletiva*, não se limitando à esfera individual, privada; iii) o direito à proteção de dados tem sua raiz na cláusula constitucional do devido processo legal[43].

Dos três pontos, esse memorial de *amicus curiae* optou, nesse momento, por focar no primeiro, buscando evidenciar o racional por trás da evolução jurisprudencial da Corte, que, em linha com uma interpretação extensiva da Constituição, efetivamente sedimenta um novo direito fundamental. É com base nesse entendimento que deve ser analisada a ADI nº 6649.

O reconhecimento, pelo Supremo Tribunal Federal, da estatura constitucional autônoma do direito à proteção de dados está diretamente relacionado a uma nítida evolução do seu entendimento sobre o que são dados pessoais e o que é uma informação que merece tutela constitucional.

De um lado, conforme abordado anteriormente, diversos ministros discorreram em seus votos sobre como mesmo os dados mais triviais hoje carregam um potencial significativo de interferência sobre a vida e os direitos dos indivíduos. Nesse sentido, o Ministro Lewandowski mencionou, a título de exemplo, como uma única linha telefônica não mais serve apenas ao propósito de permitir o contato direto entre duas pessoas, mas a diversos outros fins, inclusive como ''chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, serviços públicos e redes sociais, todos elas detentoras das mais variadas informações sobre o titular daquela linha telefônica''[44].

No mesmo sentido a citação à doutrina de Laura Schertel Mendes no voto do Ministro Gilmar Mendes: ''não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado dos danos", de modo 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 (ou no fato que quão sensíveis ou íntimos eles são)[45]".

Paralelamente às mudanças ocorridas na capacidade de processamento de dados pessoais, os votos também se apoiaram na reconceitualização da privacidade e na incorporação da ideia de autodeterminação informativa, segundo a qual o indivíduo deve ter algum nível de controle sobre o que é feito dos seus dados pessoais. Não se trata mais, nesse caso, da proteção à esfera privada do

---

[43] HILDEBRANDT, Mireille; DE VRIES, Katja. **Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology**. Routledge, 2013; KEYNES, Edward. **Liberty, property, and privacy: toward a jurisprudence of substantive due process**. Penn State Press, 2010.

[44] BRASIL. Supremo Tribunal Federal. **ADI 6393 MC-Ref / DF**. Relatora: Min. Rosa Weber. Órgão julgador: Plenário. Data de julgamento: 07/05/2020. Data de publicação: 12/11/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358850. Acesso em: 11 mar. 2021. p. 6.

[45] MENDES, Laura Schertel. **Autodeterminação informativa**: a história de um conceito. No Prelo.

cidadão, a partir de uma perspectiva negativa de ‘’não intervenção’’. Essa visão, cujo corolário imediato é a limitação da proteção constitucional ao sigilo ao conteúdo das comunicações (excluindo, por exemplo, os metadados), teve grande influência sobre a jurisprudência recente desta Corte (vide Mandado de Segurança 21.729/DF e RE 418.416-8/SC).

A ideia de autodeterminação informativa, por outro lado, ‘’revelou-se paradigmática por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso.’’ A virada hermenêutica trazida pelo julgamento da ADI 6387 foi, então, reconhecer e explicitar essa evolução, pavimentando o caminho para o reconhecimento de um direito fundamental à proteção de dados pessoais autônomo, destacado de (ainda que relacionado a) outros direitos consagrados, como intimidade e dignidade da pessoa humana.

Foi, inclusive, a construção do voto do Ministro Gilmar Mendes, que asseverou que "a afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa".

A afirmação da proteção de dados pessoais como direito fundamental autônomo (que, vale lembrar, também vem ganhando tração no Congresso Nacional, por meio da PEC 17/2019)[46] insere-se na lógica de "permanente abertura da ordem constitucional à transformação tecnológica’’[47], com a ampliação do guarda-chuva de direitos protegidos, seja por meio de alteração direta do texto constitucional, seja pelo reconhecimento de um direito implícito, deduzido interpretativamente. Caso contrário, o avançar das tecnologias e outras mudanças sociais não seria acompanhado por uma proteção jurídico-constitucional correspondente, na medida em que o próprio conteúdo dos direitos e liberdades é constantemente ressignificado à luz dos fatos.

Consciente disso, o Supremo Tribunal Federal cumpriu o papel, no julgamento da referida ADI 6387, no sentido de ampliar a sua própria esfera de atuação como garantidor de direitos

---

[46] BRASIL. Câmara dos Deputados. **PEC 17/2019**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 11 mar. 2021.

[47] BRASIL. Supremo Tribunal Federal. **ADI 6389 MC-Ref / DF**. Relatora: Min. Rosa Weber. Órgão julgador: Plenário. Data de julgamento: 07/05/2020. Data de publicação: 12/11/2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950131&ext=.pdf. Acesso em: 11 mar. 2021. Voto do Min. Gilmar Mendes (conjunto às ADIs 6.389, 6.390, 6.393, 6.388 e 6.387), p. 92.

fundamentais e guardião da Constituição Federal, calibrando o critério de avaliação de uma ofensa à privacidade e à autodeterminação informativa de acordo com as ‘’finalidades e possibilidades’’ do tratamento de dados pessoais, e não a sua natureza privada ou íntima, retomando os ensinamentos da professora Laura Schertel Mendes.

É precisamente diante desse cenário e desse acúmulo interpretativo que se deve analisar o objeto da Ação Direta de Inconstitucionalidade em discussão, isto é, ‘’a integralidade dos dispositivos estabelecidos pelo Decreto nº 10.046, de 09 de outubro de 2019’’, que ‘’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’’.

A coleta exponencial e a agregação de informações pessoais, associada ao uso de mecanismos automatizados de processamento capazes de gerar perfis precisos dos indivíduos, é responsável por um aprofundamento da assimetria informacional e de poder entre aqueles que detêm essas informações, no caso órgãos públicos, e aqueles sobre quem elas dizem respeito, os cidadãos.

O caso do compartilhamento de um conjunto de dados pessoais específico (nome, endereço e telefone) da maioria dos brasileiros com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), sem atenção à finalidade, necessidade, segurança e transparência, suscitou a virada jurisprudencial descrita até aqui. O caso que dá ensejo à presente ação reúne características semelhantes a esse precedente, além de outras que devem aprofundar o debate.

> (...) reitero, a Ministra Rosa Weber, assentar, em primeiro lugar, que a proteção de dados pessoais e autodeterminação informativa são direitos fundamentais autônomos extraídos da garantia da inviolabilidade da intimidade e da vida privada e, consectariamente, do princípio da dignidade da pessoa humana’’ (FUX, p. 55). Nesse prisma, entendo que a Medida Provisória 954/2020 desborda dos limites fixados pelos direitos fundamentais à proteção de dados e à autodeterminação informativa, extraídos da garantia da inviolabilidade da intimidade e vida privada (art. 5º, X, CF/88), do princípio da dignidade da pessoa humana (art. 1°, III, CF/88) e da garantia processual do habeas data (art. 5º, LXXII, CF/88) (FUX, p. 63)

O ministro cita o paradigmático julgamento da Lei do Censo (*Volkszählungsurteil*) em 1983 pelo Tribunal Constitucional Alemão,[48] julgado de alta relevância por reconhecer a autonomia dos direitos à proteção dos dados pessoais e à autodeterminação informacional, destacando o direito à privacidade. Para o Tribunal, a capacidade do indivíduo de autodeterminar seus dados pessoais é

[48] BUNDESVERFASSUNGSGERICHT (BVerfG). **Zitiervorschlag: BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215**. Disponível em: http://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 11 mar. 2021.

parcela fundamental do seu direito de desenvolver livremente sua personalidade. Dessa forma, a atividade de processamento dos dados pessoais deve ter limites, impondo-se "precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade " (FUX, p. 67)

No plano internacional, antes mesmo do julgamento paradigmático da Lei do Censo pelo Tribunal Constitucional Alemão, já em 1981, o Conselho Europeu para a Proteção de Dados editou a Convenção 108, de Strasbourg. Este diploma trouxe em seu art. 2º, a relevância do controle ao tratamento automatizado de dados, estipulando que a informação pessoal é considerada "qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação", ao mesmo tempo em que consagrou a imprescindibilidade de sua proteção.

Para Danilo Doneda[49], "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". É preciso ficar claro, portanto, que não se está a falar de informações insignificantes, mas da chave de acesso a dados de milhões de pessoas, com alto valor para execução de políticas públicas, é verdade, mas também com provável risco de adoção de expedientes, por vezes, dissimulados, obscuros, que possam causar desassossego na vida diária do indivíduo.

É por isso que, para muito além do mero debate sobre o sigilo comunicacional, este Tribunal deve reconhecer que a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo.

A afirmação de um direito fundamental à privacidade e à proteção de dados pessoais deriva, ao contrário, de uma compreensão integrada do texto constitucional lastreada (i) no direito fundamental à dignidade da pessoa humana, (ii) na concretização do compromisso permanente de renovação da força normativa da proteção constitucional à intimidade (art. 5º, inciso X, da CF/88) diante do espraiamento de novos riscos derivados do avanço tecnológico e ainda (iii) no reconhecimento da centralidade do Habeas Data enquanto instrumento de tutela material do direito à autodeterminação informativa.[50]

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

[49] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 358-359.
[50] Essa argumentação é desenvolvida pelo Ministro Gilmar Mendes no julgamento da cautelar deferida na ADI 6.387/DF - proposta pelo Conselho Federal da Ordem dos Advogados do Brasil - e nas ADIs 6.388/DF, 6.389/DF, 6.390/DF e 6.391/DF.

três elementos, valorização da dignidade humana, proteção constitucional à intimidade e vitalização do habeas data, é possível identificar dupla dimensão do âmbito de proteção do direito fundamental à proteção de dados.

D. A lógica procedimental de salvaguardas na Lei Geral de Proteção de Dados Pessoais e seu impacto para análise do Decreto 10.046/2019

O direito à proteção de dados pessoais não se confunde com o direito à privacidade, operando, cada um, a partir de uma lógica diversa. O direito à privacidade consiste em uma liberdade negativa, no sentido de se ver livre de interferências externas, de modo que o indivíduo se *resguarda* da vida pública, criando *obstáculos* ao acesso a dados a seu respeito que julga íntimos ou sigilosos; enquanto **o direito à proteção de dados pessoais trata de uma liberdade positiva: a *circulação* de dados pessoais de maneira *apropriada*, ou seja, com as devidas salvaguardas**[51].

O que atrai essa tutela é a caracterização dos dados como dados *pessoais*, pouco importante se são públicos ou privados. Atualmente, no que se convencionou chamar de uma sociedade e economia movida a dados, dados são utilizados – seja pelo setor privado, seja pelo setor público – para avaliar, estratificar e predizer comportamentos dos indivíduos, condicionando, cada vez mais, as oportunidades sociais a que podem ter acesso. A necessidade de salvaguardas deriva, portanto, do risco de se utilizar os dados pessoais de maneira abusiva e lesiva – como para fins discriminatórios, vigilantistas e autoritários –, prejudicando a autonomia e a participação do indivíduo na sociedade. Note-se que a proteção de dados pessoais não preconiza a retração de dados do espaço público para o espaço privado, mas sim a *circulação* de dados pessoais de forma *responsável*.

O regime de proteção de dados pessoais é, portanto, eminentemente *procedimental*.[52] Volta-se a estabelecer garantias que preservem a relação de confiança entre o titular dos dados pessoais e o agente de tratamento desses dados. Essas garantias não se traduzem em proibições ao tratamento de dados, mas, sim, na imposição de obrigações procedimentais àqueles que realizam o tratamento de dados, como deveres de transparência, segurança da informação e prestação de contas.[53]

---

[51] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[52] ZANFIR, Gabriela. Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law. In: GUTWIRTH, Serge; LEENES, Ronald. HERT, Paul de. (Eds.). **Reloading Data Protection**. Springer/Dordrecht, 2014. p. 237-257.

[53] GELLERT, Raphael; GUTWIRTH, Serge. The legal construction of privacy and data protection. **Computer Law & Security Review**, v. 29, n. 5, p. 522-530, 2013.

Nesse sentido, é importante rememorar o conceito de autodeterminação informacional, cunhado pelo Tribunal Constitucional Alemão de 1983, em conhecida decisão sobre proteção de dados pessoais.[54] A autodeterminação informacional é definida como um corolário do direito à proteção de dados pessoais[55], no sentido de assegurar ao cidadão o *controle* sobre seus dados pessoais. No entanto, **equivoca-se aquele que interpreta a decisão alemã de modo a equacionar a ideia de controle dos dados pessoais com o consentimento do titular. O conceito de autodeterminação informacional deve ser compreendido como a articulação de uma série de direitos e deveres que assegurem todas as precauções possíveis para que os riscos do tratamento de dados pessoais ao livre desenvolvimento da personalidade do indivíduo não se materializem.**[56] A esse respeito, são as considerações de Bruno Bioni:

> [...] o consentimento do titular dos dados continua a exercer um papel normativo de protagonismo, mas sob um novo roteiro que inclui a atuação de atores coadjuvantes importantes [...] o cidadão também exerce domínio sobre seus dados, se estes forem tratados de forma previsível de acordo com as suas legítimas expectativas. Portanto, o conteúdo jurídico-normativo de autodeterminação informacional vai além do consentimento. O final desse enredo proposto é a tese de que haja uma maior intervenção na economia da informação, seja para reduzir a assimetria existente entre seus agentes, seja para limitar a autonomia da vontade de quem é a sua parte (hiper)vulnerável - o titular dos dados pessoais[57].

Por isso, o ônus de tal articulação não deve recair exclusivamente sobre o indivíduo. A relação entre o titular dos dados pessoais e o agente de tratamento dos dados é de natureza *assimétrica*, o que significa que o titular é a parte mais vulnerabilizada – e por isso recebe a proteção do regime de dados pessoais. Assim, seria ilusório acreditar que o cidadão possa, por si só, fazer frente aos riscos do tratamento de seus dados pessoais[58].

É verdade que o consentimento do titular é uma base legal autorizativa do tratamento de dados pessoais, mas isso não garante o cumprimento material das demais normas de proteção de dados pessoais. **A mera existência de uma base legal não basta para que o titular dos dados seja de**

[54] HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: The population census decision and the right to informational self-determination. **Computer Law & Security Review**, v. 25, n. 1, p. 84-88, 2009.
[55] Volkszählungsurteil (BVerfGE 65, 1).
[56] Importante observar como esse direito é articulado com os valores de dignidade, autodesenvolvimento e vida cívica ativa, como elemento de sustentação de uma democracia vívida e que depende da cooperação espontânea, reflexiva, de seus membros (o que alguns autores chamam de *capacidades autonômicas*). ROUVROY, Antoinette; POULLET, Yves. The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In: GUTWIRTH, Serge et al. **Reinventing data protection?**. Springer/Dordrecht, 2009. p. 45-76.
[57] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 265-266.
[58] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

fato protegido. Isso significa dizer que o consentimento, *per se*, é insuficiente para garantir a efetiva proteção do titular dos dados, uma vez que: (i) muitas vezes o indivíduo não lê as informações sobre o uso dos dados ou não compreende o que lê e os efeitos de consentir, seja pela complexidade, seja pela sobrecarga de informações; (ii) há assimetrias de poder entre o titular e o controlador, de modo que o primeiro nem sempre é livre para consentir, muitas vezes dependendo dos serviços aos quais seus dados estão sujeitos; e (iii) o fenômeno do *Big Data* (técnica de tratamento dados em grande volume, variedade e velocidade[59]) faz com que os riscos do tratamento de dados pessoais sejam contextuais e até imprevisíveis, sequer podendo ser vislumbrados no momento inicial em que se consente com o seu tratamento[60].

Não só o consentimento, mas as demais bases legais autorizativas para o tratamento de dados também seriam insuficientes sem o respeito à lógica procedimental de salvaguardas do regime de proteção de dados, definida por meio dos princípios descritos no artigo 6º da Lei Geral de Proteção de Dados Pessoais (LGPD). A LGPD é norteada por uma interpretação sistemática de princípios, que se aplicam a todas as bases legais de tratamento de dados previstas nos artigos 7º, 11 e 23 da lei.

A base legal do legítimo interesse, por exemplo, deve ser articulada especialmente conforme os princípios de finalidade, adequação, necessidade, transparência e prestação de contas. Para que haja legítimo interesse, argumenta a doutrina[61], é preciso que: (i) o interesse perseguido seja legal, específico e real, (ii) o conjunto de dados coletados seja apto a concretizar esse interesse, (iii) o tratamento de dados seja a medida menos gravosa para se atender ao interesse perseguido de forma suficiente, e (iv) os interesses do controlador – quais sejam, a finalidade do tratamento e as implicações para a atividade que exerce – e os interesses do titular – por sua vez, as implicações do tratamento para suas liberdades e direitos fundamentais e suas expectativas legítimas – sejam ponderados, considerando a adoção de salvaguardas para minimizar o impacto do tratamento nos interesses do titular.

Não basta, portanto, dizer que o tratamento é previsto em hipótese legal. Para que se respeite materialmente o regime de proteção de dados pessoais importa *como* e *em que contexto* o

---

[59] CHEN, Hsinchun; CHIANG, Roger H. L.; STOREY, Veda C. Business intelligence and analytics: from Big Data to big impact. **MIS Quarterly**, v. 36, n. 4, p. 1165-1188, 2012. Disponível em: http://www.jstor.org/stable/41703503. Acesso em: 05 fev. 2021.

[60] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. Cap. 4, p. 160-200. In: BIONI, Bruno Ricardo et al (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

[61] MATTIUZO, Marcela; PONCE, Paula Pedigoni. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. **Internet & Sociedade**, v. 1, n. 2, p. 54-76, dez. 2020. p. 61-66; BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD:** quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: http://bit.ly/dpbrr_ebook_li. Acesso em: 05 fev. 2021.

tratamento é feito, se em atendimento ou em desacordo com os *princípios* que regem esse ecossistema da informação. Há de se analisar "as expectativas razoáveis do titular, a natureza dos dados processados e os possíveis prejuízos a serem suportados pelo titular em decorrência do compartilhamento[62]."

A primazia dos princípios da LGPD vem sendo afirmada não só pela doutrina, mas também pelo Supremo Tribunal Federal. No julgamento colegiado da medida cautelar da ADI 6.387 DF (Caso IBGE), o voto do Ministro Roberto Barroso aponta que o tratamento de dados pessoais pelo Poder Público teria sua legitimidade condicionada pelo atendimento aos princípios de finalidade, necessidade (ou minimização) e segurança:

> Portanto, eu concluo o meu voto, Presidente, com a seguinte síntese:
> 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. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Voto do Min. Roberto Barroso, p. 50).

Essas análises evidenciam que a Lei Geral de Proteção de Dados Pessoais possui, nas palavras de Ingo Woflgang Sarlet, uma concepção metainvididual, no sentido de que a autodeterminação informativa, tal como adotada na legislação brasileira a partir das teorias desenvolvidas na Alemanha, apresenta uma dupla dimensão, individual e coletiva.[63]

---

[62] ALSENOY, Brendan Van; KINDT, Els; DUMORTIER, Jos. Privacy and Data Protection Aspects of e-Government Identity Management. In: HOF, Simone Van Der; GROOTHIUS, Marga M. (Eds.). **Innovating government:** normative, policy and technological dimensions of modern government. Haia: Springer, 2011. p. 255 *apud* WIMMER, Miriam. O regime do tratamento de dados no Poder Público. Cap. 13, p. 502-534. In: BIONI, Bruno Ricardo et al (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 518.

[63] Diz o importante autor e teórico do direito constitucional brasileiro: "o direito à autodeterminação informativa – que, no concernente à sua estrutura normativa, assume a condição de princípio – também não se sobrepõe ao direito à privacidade e mesmo outros direitos especiais de personalidade, o que se verá logo adiante. Isso já se dá – mas não exclusivamente – pelo fato de o direito à autodeterminação informativa apresentar dupla dimensão individual e coletiva, no sentido de que garantida constitucionalmente não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão de seus dados pessoais, mas também – 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". SARLET, Ingo Wolfgand. Fundamentos constitucionais: o direito fundamental à proteção de dados, in: SCHERTEL MENDES, Laura; DONEDA, Danilo; SARLET, Ingo; RODRIGUE

E. O devido processo informacional como materialização da proteção de dados pessoais

Dado que o direito à proteção de dados pessoais é eminentemente procedimental,[64] segundo o qual se objetiva não a vedação do tratamento, mas sim a sua efetivação de forma adequada, **o devido processo informacional apresenta-se como um conceito fundamental para o caso em questão**.

Por devido processo informacional entende-se não só assegurar direitos aos titulares de contestação acerca do uso de seus dados, mas, também, a fixação de deveres por parte dos agentes de tratamento de dados para que a sua interferência seja justa. Trata-se tanto de "um instrumento de garantias processuais em sede judicial", quanto de "uma ferramenta de assegurar a simetria e proporcionalidade de uma forma mais ampla" sobre o tratamento de dados pessoais em relações Estado-indivíduo e privadas[65]. O devido processo informacional materializa justamente a exigência do regime de proteção de dados pessoais de garantir o controle sobre dados pessoais, no sentido de se estabelecer mecanismos (direitos e obrigações) de combate e mitigação dos riscos ao titular decorrentes do tratamento de seus dados.

O Supremo Tribunal Federal já reconheceu o devido processo informacional como corolário do direito à proteção de dados pessoais. O Ministro Gilmar Mendes, tanto em seu voto no julgamento da ADI 6.387 MC/DF (Caso IBGE), quanto na decisão monocrática por ele proferida na ADPF 695 MC/DF (Caso Denatran), afirmou que:

> A partir da tradição norte-americana, também 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. (BRASIL. Supremo Tribunal Federal. **ADI 6.387 MC / DF**. Plenário. Relator: Min. Rosa Weber. Data de julgamento: 07/05/2020. Voto do Min. Gilmar Mendes, p. 114).

JR., Otavio Luiz; BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Grupo Gen, 2021. p. 86-87.

[64] Colin Bennett argumenta que o processo de criação das FIPs (discutido no item B desta contribuição) foi calcado na ideia de salvaguardas procedimentais consistentes com a tradição estadunidense de direitos de devido processo legal (*due process*). Ver: BENNETT, Colin J. **Regulating privacy: Data protection and public policy in Europe and the United States**. Cornell University Press, 1992. p. 98.

[65] BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário?. **JOTA**, 15 jul. 2020. Disponível em: <www.jota.info/opiniao-e-analise/artigos/devido-processo-informacional-um-salto-teorico-dogmatico-necessario-15072020>. Acesso em: 20 jan. 2021.

As normas de devido processo informacional compreendem desde o desenho dos sistemas tecnológicos até o modo de tratamento dos dados em si, estabelecendo obrigações positivas de conformidade aos princípios de proteção de dados pessoais, em especial aos de segurança, transparência e prestação de contas. Nesse sentido, estariam medidas como habilitar a personalização das configurações de privacidade e proteção de dados de uma plataforma, abrir os seus códigos, produzir relatório de impacto à proteção de dados pessoais e implementar mecanismos de autenticação dos dados coletados. Faz parte do âmbito do devido processo informacional, também, a "cautela na própria formação de bancos de dados, pretendendo garantir qualidade, exatidão, clareza e atualização dos elementos que os compõem"[66].

A instituição do Decreto 10.046/2019 falha em estabelecer critérios de "devido processo informacional". De um lado, amplia demasiadamente as capacidades dos gestores de aumentar as bases de dados constantes da "base integradora"[67], incluindo os "dados biométricos", entendidos, na linguagem do Decreto, como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar".

Por outro lado, cria uma sistemática pobre de salvaguardas para o *uso compartilhado* dessas informações dentro da administração pública. O Decreto aposta em mecanismos de compartilhamento de dados - entendido como "recurso tecnológico que permite a integração e a comunicação entre aplicações e serviços do recebedor de dados e dos órgãos gestores de dados, tais como serviços web, cópia de dados, lago de dados compartilhado e plataformas de interoperabilidade" - porém deixa de construir testes adequados para o regramento do uso compartilhado.

A lógica de categorização dos tipos de acesso e de compartilhamento (entre *amplo*, *restrito* e *específico*, tal como previsto nos artigos 11 a 15 do Decreto 10.046/2019), somada aos poderes concedidos ao Comitê Central de Governança de Dados, é insuficiente para uma concepção de um *compartilhamento justo* ou uma *interface de interoperabilidade justa*. O elemento de justiça (*fairness*) é a construção de um teste que possa atrelar o uso compartilhado a uma razão de ordem pública legítima e adequada, a partir de um procedimento transparente e auditável pelos cidadãos.

---

[66] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. Cap. 4, p. 160-200. In: BIONI, Bruno Ricardo et al (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 181.

[67] "Base integradora" é base de dados que integra os atributos biográficos ou biométricos das bases temáticas, nos termos do Decreto 10.046/2019.

F. O tratamento de dados pessoais é uma questão de interesse público e a favor do Poder público: o falso antagonismo

A existência de salvaguardas procedimentais, em conformidade com os princípios norteadores da proteção de dados pessoais, é crucial para a realização de um tratamento de dados justo. Essa necessidade deve ser redobrada em um contexto em que o poder público atua como agente de tratamento de dados, uma vez que **a relação entre o Estado e o indivíduo é marcada por significativas assimetrias de poder e as consequências de um tratamento ilegítimo podem impactar negativamente toda a sociedade**.

Tal preocupação remonta à década de 1970, época em que surgiram as primeiras legislações de proteção de dados pessoais. Estas tinham por objetivo impor limites ao Estado, que pretendia promover a centralização de bases de dados pessoais dos cidadãos. Esse foi o caso da Alemanha, com a Lei de Hesse de 1970, da Suécia, com o *Datalagen*, Ato de Dados Sueco de 1973, e dos Estados Unidos, com o *Privacy Act* de 1974[68].

A relação Estado-cidadão é essencialmente desigual. O Estado detém o monopólio da força coercitiva e controla o acesso dos indivíduos a bens básicos. Nesse sentido, a coleta, o uso e o tratamento dos dados pessoais dos cidadãos pelo Poder Público no exercício de suas atribuições trazem, por si só, sérios riscos aos direitos e liberdades fundamentais dos cidadãos. A partir do acesso a tais dados, o Estado poderia obter informações sensíveis que o permita vigiar, controlar e discriminar certos grupos da sociedade. A centralização de bases de dados pelo Poder Público agrava ainda mais esse cenário, porque aumenta a capacidade do agente de tratamento de cruzar diversos dados antes isolados e, então, extrair informações e correlações e perfilhar indivíduos e grupos. Concentrar dados pessoais também é mais arriscado do ponto de vista da segurança da informação, uma vez que todos os esforços de acesso não autorizado seriam direcionados para uma única base. Se a tentativa de acesso à base for bem-sucedida, por um lado, a recompensa aos invasores é valiosa; por outro, o estrago causado aos titulares é extremamente gravoso. Ainda, a centralização de diversos dados de origens distintas ocorre associada à circulação ilimitada de dados dentre os entes do Poder Público, permitindo que dados coletados para uma finalidade específica sejam utilizados para outra diversa[69].

Assim, para que a relação Estado-cidadão seja justa e mantenha a confiança necessária para o bom, eficiente e democrático funcionamento da sociedade, é preciso que o Poder Público

---

[68] WIMMER, Miriam. O regime do tratamento de dados no Poder Público. Cap. 13, p. 502-534. In: BIONI, Bruno Ricardo et al (Coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. p. 506.

[69] ABREU, Jaqueline de Souza. O compartilhamento de dados pessoais no Decreto n. 8.789/16: um Frankenstein de dados brasileiro?. **JOTA**, 08 jul. 2016. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-compartilhamento-de-dados-pessoais-no-decreto-n-8-789 16-um-frankenstein-de-dados-brasileiro-08072016>. Acesso em: 20 jan. 2021.

atue de forma precaucionária, isto é, em conformidade com os princípios norteadores da proteção de dados pessoais.

A LGPD (Lei n. 13. 709/2018) determina as diretrizes para a proteção de dados pessoais no âmbito do setor público, estabelecendo as bases legais, bem como as regras e exceções de incidência. Como sintetizado por Miriam Wimmer[70], a legislação fornece duas bases legais que legitimam o tratamento de dados pessoais pelo Poder Público: (i) a *execução de políticas públicas*, positivada nos artigos 7º e 11 e (ii) o cumprimento de atribuições institucionais, especificada no artigo 23, como a *execução de competências ou atribuições legais do serviço público.*

No artigo 4º, III da LGPD, o legislador elencou atividades do setor público sobre as quais não incidem a LGPD. São elas as atividades realizadas para fins exclusivos de (a) segurança pública; (b) defesa nacional; (c) segurança do Estado; ou (d) atividades de investigação e repressão de infrações penais. Inobstante essas exceções previstas, há salvaguardas relevantes a serem observadas, também positivadas pela lei[71].

O parágrafo 1º do artigo 4º da lei estabelece que: "O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever **medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, observados o devido processo legal, **os princípios gerais de proteção** e os direitos do titular previstos nesta Lei." (grifos nossos). Ou seja, o legislador deixou claro que, mesmo as atividades que têm sua incidência material excluída da aplicação da lei, têm de observar as normas estruturais de de proteção de dados[72].

Nesse sentido, para que o Poder Público possa legitimamente tratar dados pessoais dos cidadãos, deve *sempre* articular a finalidade específica, a adequação e a necessidade do tratamento no que tange o atendimento ao interesse público - bem como observar os demais princípios da LGPD. Tais requisitos têm de ser observados *ainda que* o tratamento de dados enquadre-se em quaisquer uma das atividades elencadas no artigo 4º, III da LGPD.

---

[70] WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **Revista do Advogado**: Lei Geral de Proteção de Dados Pessoais, n. 144, p. 126-133, nov. 2019.

[71] "[...] por força de suas especificidades, há determinados tipos de atividades públicas que frequentemente são submetidas a uma lógica de excepcionalidade no que se refere às regras de proteção de dados pessoais. Trata-se, tipicamente, daquelas relacionadas a uma das funções mais básicas do Estado. [...] É importante notar que a exclusão de tais atividades do escopo da LGPD, com indicação da necessidade de tratamento do tema por legislação específica, se dá com a salvaguarda de certas premissas. Nos termos da lei, a legislação específica deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, devendo ser observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na própria LGPD." WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades.**Revista do Advogado**: Lei Geral de Proteção de Dados Pessoais, n. 144, p. 126-133, nov. 2019.

[72] WIMMER, Miriam. Proteção de dados pessoais no Poder Público: incidência, bases legais e especificidades. **Revista do Advogado:** Lei Geral de Proteção de Dados Pessoais, n. 144, p. 126-133, nov. 2019.

O interesse público[73] não pode ser utilizado como justificativa universal para legitimar o tratamento inadequado de dados pessoais. Especificamente, é errôneo justificar, por meio do interesse público, todo e qualquer tratamento de dados chefiado pelo setor público, por duas razões fundamentais: (i) o atendimento ao interesse público tem de ser lido em consonância com os demais princípios positivados na legislação de proteção de dados e (ii) a averiguação da necessidade e da proporcionalidade do tratamento não pode ser feita na lógica equivocada do interesse público como antagônico à privacidade e à proteção de dados.

No que se refere ao primeiro ponto, o interesse público não existe de maneira isolada, mas deve ser lido conjuntamente com outros princípios. Nesse sentido, no contexto europeu, os princípios de legalidade, do tratamento justo e da transparência aplicam-se a *todas* as formas de tratamentos de dados[74]. Conforme as diretrizes europeias, o princípio da legalidade implica na necessidade de uma justificativa (base legal) para o tratamento de dados pessoais.

O Regulamento Europeu de Proteção de Dados Pessoais prevê o que pode ser considerado um tratamento lícito em seu artigo 6º (1). A mesma racionalidade está positivada no artigo 7º da Lei Geral de Proteção de Dados no Brasil. O tratamento justo baseia-se na lógica da relação assimétrica entre o controlador de dados pessoais e seu titular, estabelecendo como ônus do controlador a publicação das operações de tratamento realizadas, a delimitação de sua base legal e o registro das razões da escolha de cada uma das bases legais atribuídas às operações de tratamento de dados. O princípio da transparência, por sua vez, estabelece ao controlador a obrigação de informar o titular sobre como seus direitos estão sendo tratados, bem como apresentar as finalidades de seu tratamento antes de qualquer operação. Esse princípio está elencado no artigo 6º, VI da LGPD.

Ou seja, não basta o setor público justificar qualquer tratamento de dados pessoais por meio do atendimento a um interesse público se não houver, concomitantemente, respeito aos princípios norteadores e basilares de toda a seara de privacidade e proteção de dados pessoais. Especificamente, se for comprovado o interesse público, mas não houver respeito aos princípios

---

[73] O interesse público, de acordo com Autoridades de Proteção de Dados Pessoais, possui um caráter volátil. O teste é necessário para identificar interesses públicos apropriados, caso a caso. A ideia é bastante incerta. A ICO, por exemplo, define interesse público como "a wide range of values and principles relating to the public good, or what is in the best interest of society. Thus, for example, there is a public interest in transparency and accountability, to promote public understanding and to safeguard democratic processes. There is a public interest in good decision-making by public bodies, in upholding standards of integrity, in ensuring justice and fair treatment for all, in securing the best use of public resources and in ensuring fair commercial competition in a mixed economy". ICO, **What are the substantial public interest conditions?**. London: ICO, 2021. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-substantial-public-interest-conditions/. Acesso em 03 mar. 2021.

[74] European Union. Handbook on European Data Protection Law. 2018 edition. Handbook / FRA, European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018.: Disponível em: <http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law>. p. 19.

elencados no artigo 6º da LGPD, o tratamento é ilegítimo. São critérios cumulativos e não excludentes. Assim, será que um tratamento de dados que não respeite os princípios basilares da proteção de dados pessoais, ainda que realizado pelo Poder Público, estaria, de fato, servindo ao interesse público?

Isso leva ao segundo ponto, que trata da razão pela qual é errôneo justificar, unicamente por meio do interesse público, todo e qualquer tratamento de dados por parte do setor público: o interesse público não é antagônico à privacidade e à proteção de dados. É fundamental fugir desta armadilha ao se averiguar a proporcionalidade e necessidade do tratamento dos dados. Trata-se de um falso antagonismo, como já abordado pelo Ministro Gilmar Mendes, na decisão liminar proferida no âmbito da ADPF 695[75]:

> A discussão sobre privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados[76].

Nesse sentido, um desdobramento prejudicial ao interesse público foi alertado no campo de políticas públicas educacionais, pelo ministro Luís Roberto Barroso, nos autos do Mandado de Segurança n. 36.150 MC, em que o relator deferiu a cautelar para cassar determinação do Tribunal de Contas da União (TCU), que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família[77]. Na decisão o ministro alerta para a existência de um interesse público, de toda a coletividade, no sentido da importância de uma política pública educacional baseada em

---

[75] Liminar indeferida por conta da revogação do Acordo entre Denatran e Serpro, restando ausentes os pressupostos para a concessão da tutela de urgência, mas " [...] resta pendente de análise, por este STF, a alegação de que as disposições do Decreto no. 10.046, de 9 de outubro de 2019 violam in abstracto o disposto no art. 5o, caput e incisos X e XII, da Constituição Federal", uma vez que "[...] o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (art. 5o, caput e incisos X, da Cons tituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea." Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693Acesso em: 19/01/2021. p. 47.

[76] Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021. p. 26.

[77] Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP= TP & docID= 753005479 & prcID=5938693 Acesso em: 19/01/2021.

dados. Por isso, diz o voto, a política pública em si já era boa, mesmo que o titular dos dados considere que o INEP traiu a confiança no que se refere à política de uso de tais dados.

> É plausível a alegação de que a transmissão desses dados para finalidade diversa: (i) subverte a autorização daqueles que concordaram em prestar as declarações; e (ii) coloca em risco a capacidade do INEP de pesquisar e monitorar políticas públicas.
> (...)
> é plausível a alegação de que a franquia desses dados quebra a confiança no órgão responsável pela pesquisa por violação do sigilo estatístico (..) com efetivo prejuízo ao monitoramento das políticas públicas de educação")."

Essa falsa dicotomia nasce de um entendimento incorreto de que privacidade e proteção de dados são, única e exclusivamente, direitos individuais. Se entendidos dessa maneira, a ponderação acerca da legitimidade do tratamento feito pelo Poder Público tornar-se-ia enviesada. Especificamente, por meio de tal lógica equivocada, ao se buscar saber se determinado tratamento de dados é legítimo ou não, por meio de um sopesamento entre (i) a necessidade do tratamento de dados que beneficie o interesse público e (ii) os direitos de proteção de dados pessoais, tem-se, simplificadamente, a seguinte equação: (i) interesse público vs. (ii) interesse privado. Ou seja, ao rejeitar a abordagem focada em privacidade e proteção de dados pessoais como parte do interesse público, sempre será possível que controladores do setor público legitimem a coleta e tratamento de dados, uma vez que esta sempre será considerada necessária e proporcional[78].

Por óbvio, essa balança tende, quase sempre, a privilegiar o interesse público e, consequentemente, acaba por legitimar qualquer tratamento de dados capitaneado pelo setor público sob a justificativa do interesse público. Em outras palavras, a derrota da privacidade e da proteção de dados é quase certa, se esses direitos forem enquadrados como individuais, porque é difícil de imaginar situações nas quais o direito individual se sobreporia ao interesse coletivo[79].

---

[78] O Ministro Gilmar Mendes também já reconheceu essa armadilha conceitual ao proferir a decisão liminar no âmbito da ADPF 695: "Como bem destacado por Guilian Black e Leslie Stevens, pesquisadores britânicos dedicados a essa temática, 'se a privacidade for tratada simplesmente como um direito ou interesse individual, sempre será possível para o setor público controlar dados para suas finalidades públicas, já que isso será sempre reputado como necessário e proporcional'" (tradução livre). Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[79] "A tentativa de balancear interesses (nomeados como interesses públicos) contra direitos e liberdades fundamentais é insatisfatório e desigual." (tradução livre) BLACK, Gillian; STEVENS, Leslie. Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest. **Scripted**, v. 10, n. 1, 2013.

Mas essa é uma **equação falsa**: a privacidade e a proteção de dados pessoais têm valor social e não apenas individual. Fundamentalmente, porque possuem um núcleo elementar de afinidade com a autonomia individual e com a dignidade da pessoa humana, integrando a lógica da democracia como um todo[80]. Respeitar tais direitos evita não somente danos individuais, mas, sobretudo, o esgarçamento da confiança coletiva no Estado enquanto custodiador dos seus dados. Ou seja, sua proteção está manifestamente incluída no interesse público e, em última análise, é favor do Estado para que ele corresponda ao voto de confiança que lhe foi dado, isto é, para que mantenha a sua posição de fiduciário da informação de toda a coletividade[81].

Nesse sentido, a privacidade e a proteção de dados pessoais podem ser vistas como direitos privados, mas mantêm-se, concomitantemente, na categoria do interesse público e com uma dimensão coletiva. Um direito não deve ser visto exclusivamente como um direito individual, simplesmente porque protege um indivíduo: ele ainda pode ter benefícios e implicações mais amplas para a sociedade como um todo[82].

O interesse público, portanto, não pode ser arguido como um supertrunfo à privacidade e à proteção de dados pessoais, justamente porque elas integram, também, a categoria de interesse público. Dito de outra maneira, uma boa concepção de interesse público deve englobar o respeito à proteção de dados pessoais. Resta clara, portanto, "a necessidade de se conferir uma abordagem comunitária e institucional ao direito à proteção de dados pessoais, evitando-se que este valor sempre sucumba diante da invocação do interesse público"[83].

G. A necessidade de um teste de proporcionalidade no desenho do Decreto 10.406/2019

Por esse ponto de vista, a equação da proporcionalidade/necessidade passa a ser reescrita como *interesse público vs. interesse público,* o que implica a necessidade de um sopesamento **efetivo,** cujo resultado só se sabe após um balanceamento casuístico - e não de antemão. Esse

---

[80] "É corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais que os governos tratem o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais." Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[81] BLACK, Gillian; STEVENS, Leslie. Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest. **Scripted**, v. 10, n. 1, 2013.

[82] Idem.

[83] Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

balanceamento torna-se, por óbvio, muito mais complexo, mas os já citados Gillian Black e Leslie Stevens formularam um teste de proporcionalidade que pode - e deve - ser utilizado como método de averiguação acerca da necessidade e proporcionalidade de determinado tratamento de dados capitaneado pelo Poder Público.

A decisão monocrática do Ministro Relator Gilmar Mendes sobre a medida cautelar da ADPF 695/DF (Caso Denatran) traz a formulação de um teste de proporcionalidade que condiciona a legitimidade do tratamento de dados pessoais pelo Poder Público no caso concreto ao atendimento aos princípios de adequação, necessidade e proporcionalidade em sentido estrito:

> Como bem destacado em artigo escrito por Gillian Black e Leslie Stevens, a proporcionalidade tem sido o principal parâmetro utilizado no Direito Europeu para a aferição da constitucionalidade do tratamento de dados no setor público. Os autores desenvolvem uma aplicação trifásica desse teste, o qual reflete as tradicionais fases de valoração da adequação, necessidade e proporcionalidade em sentido estrito. (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).
>
> Do ponto de vista da ***necessidade, cumpre*** avaliar se o processamento ou compartilhamento dos dados pelos órgãos converge para um legítimo objetivo de política pública ou para o exercício de uma obrigação legal dos órgãos públicos envolvidos.
>
> Do ponto de vista da ***adequação***, cumpre avaliar quais os riscos envolvidos no processamento dos dados em questão e qual a possibilidade de dano aos indivíduos titulares. Também nessa fase, revela-se necessário entender se a medida adotada é a menos invasiva possível para o resultado visado.
>
> Já na aferição da ***proporcionalidade*** em sentido estrito, o que deve ser examinado é se o interesse público atinente a esse processamento é superior ao interesse público da coletividade envolvido na vulneração da proteção dos dados pessoais. (BRASIL. Supremo Tribunal Federal. **ADPF 695 MC / DF**. Decisão monocrática. Relator: Min. Gilmar Mendes. Data de julgamento: 24/06/2020. Voto do Min. Gilmar Mendes, p. 40. Grifos no original).

Esse método afasta um conceito adversarial, segundo o qual a privacidade e a proteção de dados pessoais são obstáculos ao tratamento de dados por parte do Poder Público. Baseia-se, por sua vez, em uma abordagem cooperativa, pela qual se busca melhorar a privacidade ao mesmo tempo em que se utiliza de dados pessoais para a elaboração e prestação de serviços e políticas

públicas datificadas.[84] Essa abordagem é principiológica, o que faz com que as decisões tenham de levar em conta valores fundamentais.

O teste elaborado pelos autores passou pelo crivo do STF na já citada liminar proferida pelo Ministro Gilmar Mendes, no âmbito da ADPF 695[85], e consiste em um guia mais objetivo, na tentativa de assegurar a evolução da datificação Poder Público, ao mesmo tempo que os direitos e interesses dos titulares dos dados não sejam sacrificados em prol de uma concepção corrompida e unilateral do interesse público. Reproduzimos as três fases do referido teste:

O Teste de Proporcionalidade proposto por BLACK, G. e STEVENS, L. (2013) para facilitar a averiguação da necessidade e proporcionalidade de tratamento de dados feitos pelo Poder Público[86]:

[84] Sobre o conceito de datificação em políticas públicas, ver KUCH, Declan; KEARNES, Matthew; GULSON, K. The promise of precision: datafication in medicine, agriculture and education. **Policy Studies**, v. 41, n. 5, p. 527-546, 2020.

[85] A tradução do Ministro Gilmar Mendes, na íntegra, no âmbito da Liminar da ADPF 695: "Do ponto de vista da necessidade, cumpre avaliar se o processamento ou compartilhamento dos dados pelos órgãos converge para um legítimo objetivo de política pública ou para o exercício de uma obrigação legal dos órgãos públicos envolvidos. Do ponto de vista da adequação, cumpre avaliar quais os riscos envolvidos no processamento dos dados em questão e qual a possibilidade de dano aos indivíduos titulares. Também nessa fase, revela-se necessário entender se a medida adotada é a menos invasiva possível para o resultado visado. Já na aferição da proporcionalidade em sentido estrito, o que deve ser examinado é se o interesse público atinente a esse processamento é superior ao interesse público da coletividade envolvido na vulneração da proteção dos dados pessoais. A fim de orientar a aplicação dessas fases, Gillian Black e Leslie Stevens orientam a formulação dos seguintes quesitos que devem ser respondidos pelo controlador para se verificar se o método de tratamento é proporcional para consecução dos objetivos: i. O tratamento proposto dos dados pessoais é o meio menos intrusivo para atingir o objetivo do órgão público? ii. O processamento está de acordo com os demais princípios de proteção de dados incluindo, criticamente, o terceiro princípio de proteção de dados, o qual requer que os dados pessoais processados não devem ser excessivos?; iii. A anonimização pode ser utilizada e, em caso afirmativo, a técnica proposta é considerada efetiva? iv. A proposta de processamento foi aprovada por um órgão competente? v. Foi realizada uma avaliação de impacto na privacidade para avaliar e mitigar os riscos inerentes ao processamento em questão? vi. Existe um interesse público identificável no processamento dos dados pessoais? vii. Existe um interesse público identificável em fornecer ao público serviços relevantes?" Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[86] Além da segurança jurídica que nasce de um método objetivo, o teste possui alguns benefícios fundamentais: (1) faz com que o controlador tenha de identificar, por meio dos passos 1 e 2, todos os interesses em jogo; (2) faz com que os controladores *e* indivíduos tenham uma maior confiança no processo de tomada de decisão, porque existe um método, gerando maior confiança nos próximos tratamentos e (3) põe fim ao favorecimento injustificado de tratamentos de dados pelo setor público, porque requer que o controlador faça uma análise que considere, também, os interesses dos indivíduos e sua proteção como algo de interesse público.

Passo 1: Bases legais da coleta e tratamento: 1. *O tratamento tem um objetivo legítimo? Isto é: enquadra-se em alguma das bases legais estabelecidas pela Lei Geral de Proteção de Dados?* *O tratamento está em consonância com os princípios de proteção de dados?*
Passo 2: Identificação dos dados pessoais, focando nos interesses do indivíduo. *Quais dados pessoais estão envolvidos neste tratamento? São dados sensíveis? Quais são os riscos envolvidos nesse uso? Quais as probabilidades resultar em um dano ao indivíduo?*
Passo 3: Sopesamento *O interesse público visado pelo tratamento está em conformidade com as normas de proteção de dados pessoais, a ponto de ser sopesado e mitigar possíveis riscos aos interesses individuais do titular dos dados?* *i. O tratamento proposto dos dados pessoais é o meio menos intrusivo para atingir o objetivo do órgão público?* *ii. O processamento está de acordo com os demais princípios de proteção de dados incluindo, criticamente, o terceiro princípio de proteção de dados, o qual requer que os dados pessoais processados não devem ser excessivos?;* *iii. A anonimização pode ser utilizada e, em caso afirmativo, a técnica proposta é considerada efetiva?* *iv. A proposta de processamento foi aprovada por um órgão competente?* *v. Foi realizada uma avaliação de impacto na privacidade para avaliar e mitigar os riscos inerentes ao processamento em questão?* *vi. Existe um interesse público identificável no processamento dos dados pessoais?* *vii. Existe um interesse público identificável em fornecer ao público serviços relevantes?*

Conforme explicam os autores, respostas positivas às perguntas de cada um dos passos são um indicativo de que o processamento é legítimo. Respostas negativas, por outro lado, indicam que o interesse público será melhor servido se os dados em questão forem protegidos e, assim, não coletados nem tratados. Assim, conforme se verifica pela aplicação do teste, a governança no compartilhamento de dados estabelecida pelo Decreto 10.046/2019, bem como o Cadastro Base Cidadão, não parecem ser necessárias ou proporcionais, configurando tratamento de dados ilegítimo por parte do Poder Público.

Frise-se que o regime de proteção de dados não é um obstáculo ao tratamento de dados pelo Poder Público, mas apenas uma procedimentalização a qual deve estar sujeito. Dito de outra forma, a LGPD não é um empecilho à datificação da Administração Pública, nem mesmo ao aumento de sua eficiência.

H. O cruzamento entre os princípios da proteção de dados e os princípios constitucionais da administração pública

Seguir as normas de proteção de dados (e.g., a LGPD) é um instrumento necessário e que favorece o uso de dados pelo Poder Público**.** Quando esse ponto de vista conciliatório e instrumental é adotado, somado a concepção fundamental de que a proteção de dados pessoais integra a seara de interesses públicos, "[...] não há dúvidas de que relevantes princípios constitucionais estão em jogo quando se discutem os limites do tratamento de dados pelo Poder Público, tais como o princípio da eficiência da Administração Pública[87]". **Os princípios da LGPD se aplicam ao Poder Público em *complemento* aos princípios constitucionais da Administração Pública**.

Ao nos distanciarmos da falsa dicotomia da Administração como detentora de interesses públicos e da LGPD como protetora de interesses individuais, a releitura dos princípios da administração pública à luz dos princípios de proteção de dados pessoais é quase natural. O entendimento da legalidade dessa harmonização principiológica, inclusive, já foi reconhecido pelo STF[88], em decisão monocrática proferida pela Ministra Cármen Lúcia, na Suspensão de Liminar 1.103 MC e na decisão monocrática do Ministro Roberto Barroso, no Mandado de Segurança 36.150 MC[89].

---

[87] Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[88] "Convém destacar que essa visão de compatibilização dos interesses da Administração Pública com a defesa de garantias individuais na temática da proteção de dados pessoais no Poder Público não é de todo estranha à jurisprudência do STF. Em pelo menos duas ocasiões, o Tribunal impôs limitações a um modelo de fluxo multidirecional e irrestrito do compartilhamento de dados entre órgãos e instituições públicas." Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[89] "Destaca-se, nesse sentido, decisão da lavra da então presidente Ministra Cármen Lúcia na Suspensão de Liminar 1.103 MC, em que Sua Excelência determinou que o IBGE se abstivesse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças, na área urbana do município de Bauru/SP, desprovidas de registro de nascimento e, por conseguinte, da proteção do Estado e da sociedade. Nessa decisão, a Min. Cármen Lúcia afirmou a necessidade de conciliação dos valores constitucionais em jogo ao pontuar que: 'O dever de sigilo proporciona segurança a quem presta as informações e contribui para a confiabilidade das pesquisas efetuadas. Recepção das normas que estabelecem o sigilo das informações colhidas pelo IBGE (art. 2o, § 2o, do Decreto-lei n. 16111967 e parágrafo único, do art. 1o, da Lei no 5.534/1968) pela Constituição Federal de 1988. IV. Quando princípios fundamentais da Constituição conflitam entre si, a questão deve ser analisada tendo em vista o caso concreto, respeitados os

Isto posto, mesmo que a **eficiência administrativa** esteja positivada constitucionalmente, não é, por si só, uma legitimadora de todo e qualquer tratamento de dados pelo Poder Público. Nesse sentido, não basta o Decreto 10.046/2019 elencar como uma de suas finalidades "aumentar a qualidade e a eficiência das operações internas da administração pública federal" para justificar uma lógica de compartilhamento de dados no âmbito da administração pública, bem como o Cadastro Base do Cidadão. Há impedimentos para tanto não só no âmbito da LGPD, como na própria racionalidade constitucional da Administração Pública.

A eficiência administrativa (artigo 37 da Constituição Federal) tem um limite inerente à própria lógica principiológica da administração pública. Segundo Odete Medauar, em sua obra "Direito Administrativo Moderno" esclarece que, apesar de a eficiência ser o princípio norteador da atuação da Administração Pública, determinando que esta tenha de agir de modo célere e preciso, produzindo resultados que satisfaçam às necessidades da população, "o princípio da eficiência vem suscitando entendimento errôneo no sentido de que, em nome da eficiência, a legalidade será sacrificada. Os dois princípios constitucionais da Administração devem conciliar-se, buscando esta atuar com eficiência, dentro da legalidade[90]."

Assim, a eficiência não pode ser uma justificativa para toda e qualquer ação da administração porque é, sempre, limitada pela **legalidade**. Se a ação administrativa consistir em tratamento de dados, há, ainda, as limitações da LGPD, já elencadas ao longo desta peça (lógica protetiva dos titulares, princípios de proteção de dados e o dever de comprovação da necessidade e proporcionalidade do tratamento em questão). Tais limitações à eficiência dialogam, pois indicam o caminho a ser seguido para que ela seja buscada sempre ao lado da legalidade e do respeito aos direitos fundamentais.

O princípio da eficiência administrativa, inclusive, conversa diretamente com o princípio da **necessidade**, previsto no artigo 6º, III da LGPD. A necessidade, na lógica da proteção de dados pessoais, consiste em uma limitação à coleta e ao tratamento de dados como somente ao mínimo

---

valores supremos consagrados na ordem constitucional. Com base no juízo de ponderação, busca-se identificar em qual dimensão deve um direito fundamental preponderar quando contraposto a outro direito também fundamental. Para isso, deve-se recorrer aos princípios instrumentais da razoabilidade e da proporcionalidade, implícitos na Constituição, e sopesar os valores protegidos pelas normas em conflito. Não se trata de eliminar um direito para fazer "predominar exclusivamente outro, mas sim de conciliar os bens jurídicos em conflito e harmonizá-los com os princípios consagrados no sistema jurídico constitucional'. No mesmo sentido, cumpre citar ainda decisão recente de lavra do Ministro Luís Roberto Barroso, nos autos do Mandado de Segurança 36.150 MC, em que o relator deferiu a cautelar para cassar determinação do Tribunal de Contas da União (TCU), que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família." Supremo Tribunal Federal. **Ação de Descumprimento de Preceito Fundamental n. 695/DF,** Relator Ministro Gilmar Mendes. Decisão Monocrática 24/06/2020. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=753005479&prcID=5938693 Acesso em: 19/01/2021.

[90] MEDAUAR, Odete. **Direito Administrativo moderno**. 21. ed. Belo Horizonte: Fórum, 2018. p. 125-126.

necessário para a realização da finalidade pretendida. A eficiência verifica-se justamente nesse ponto de se coletar somente o que se vai utilizar: se o que se busca com uma administração eficiente são resultados rápidos e precisos, coletar mais dados do que o estritamente necessário é um obstáculo à essa celeridade desejada.

Além disso, se eficiência pode ser entendida como uma contraposição não só à lentidão, mas também ao descaso, à negligência e à omissão[91], faz parte da eficiência administrativa procurar ativamente meios para se evitar quaisquer danos à população. Quanto mais dados se coleta - ou seja, quanto maior a base de dados que se cria[92] - maior o dano ao erário no caso de algum vazamento ou incidente de segurança. A necessidade, portanto, é um princípio que anda de mãos dadas com a eficiência: ao se obrigar o controlador público a coletar e tratar efetivamente somente o que será necessário para atingir a finalidade visada, diminui-se as chances de danos ao erário público.

Há, ainda, outros princípios que exemplificam essa harmonização entre o disposto na LGPD e Administração Pública. O princípio da **moralidade** administrativa, por exemplo, relaciona-se diretamente com o princípio da **finalidade**, positivado no artigo artigo 6º, I da LGPD como: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". A moralidade administrativa, por sua vez, tem uma de suas facetas atrelada ao desvio de finalidade. Ou seja, "a imoralidade administrativa estaria na intenção do agente[93]".

Assim, se a LGPD prevê que, para ser legítima, toda e qualquer coleta e tratamento de dados pessoais deva ter finalidade específica e explícita, e a imoralidade administrativa pune o desvio de finalidade do agente público, é possível concluir, por meio de uma harmonização entre os princípios, que o controlador público que fugir da finalidade inicial de determinada coleta e tratamento de dados incorre em sanções administrativas, por desrespeito à moralidade administrativa, e também, sanções da seara de proteção de dados pessoais.

Há, inclusive, previsão expressa no próprio artigo 6º, I da LGPD, que termina com a proibição de tratamento posterior incompatível com as finalidades iniciais. O artigo 23, situado no Capítulo do Tratamento de Dados Pessoais pelo Poder Público da LGPD, também prevê, explicitamente, que: "o tratamento de dados pessoais pelas pessoas jurídicas de direito público [...] 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

---

[91] MEDAUAR, Odete. **Direito Administrativo moderno**. 21. ed. Belo Horizonte: Fórum, 2018. p. 125-126.
[92] Como no caso do Cadastro Base Cidadão.
[93] DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 33. ed. Rio de Janeiro: Forense, 2020. p. 25.

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". (grifos nossos)

Para citar mais um exemplo, os princípios da **publicidade** (artigo 37 da Constituição Federal) e da **transparência** (artigo 6º, VI da LGPD). Administrativamente, "o princípio da publicidade [...] exige a ampla divulgação dos atos praticados pela Administração Pública, ressalvadas as hipóteses de sigilo previstas em lei[94]." No âmbito da proteção de dados pessoais, a transparência consiste na 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.

A lógica, como se depreende, é a mesma: a democratização dos procedimentos públicos.

> O tema da transparência ou visibilidade, também tratado como publicidade da atuação administrativa, encontra-se associado à reivindicação geral de democracia administrativa. A partir da década de 50, acentuando-se nos anos 70, surge o empenho em alterar a tradição do "secreto" predominante na atividade administrativa. A prevalência do "secreto" na atividade administrativa mostra-se contrária ao caráter democrático do Estado. A Constituição de 1988 alinha-se a essa tendência de publicidade ampla a reger as atividades da Administração, invertendo a regra do segredo e do oculto que predominava. O princípio da publicidade vigora para todos os setores e todos os âmbitos da atividade administrativa[95].

Vê-se, por meio desses três exemplos, que o diálogo principiológico entre Administração Pública e LGPD está longe de ser adversarial: os princípios se complementam. Reforça-se, assim, a visão de que a LGPD não existe como um obstáculo à Administração Pública, mas como um instrumento para seu funcionamento legal.

III. PEDIDOS

Ante todo o exposto, na qualidade de *amicus curiae*, requer-se seja concedida a medida liminar pleiteada e, ao final, que a presente demanda seja julgada procedente para se reconhecer que as regras gerais de compartilhamento de dados previstas nos artigos 5ª a 15, do Decreto

[94] DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 33. ed. Rio de Janeiro: Forense, 2020. p. 14.
[95] DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 33. ed. Rio de Janeiro: Forense, 2020. p. 15.

10.046/2019 e o desenho institucional do Cadastro Base do Cidadão, previsto nos artigos 16 e 17 da referida norma, não são compatíveis com o direito fundamental à proteção de dados pessoais, por não preverem salvaguardas contra a utilização abusiva de dados pessoais, não garantirem a legitimidade do uso compartilhado dos dados e permitirem acesso a dados pessoais para além da extensão mínima necessária para a realização dos objetivos da norma.

Por fim requer-se seja conferida a possibilidade de sustentação oral e que os subscritores da presente sejam previamente intimados da realização do ato;

Termos em que,

Pede-se deferimento.

São Paulo, 08 de abril de 2021.

BRUNO RICARDO BIONI

OAB/SP nº 316.083

RAFAEL AUGUSTO FERREIRA ZANATTA

OAB/SP nº 311.418

MARIANA MARQUES RIELLI

OAB/SP nº 408.049

IZABEL SAENGER NUÑEZ

OAB/RJ nº 232.503

PEDRO JOSÉ NASSER SALIBA

OAB/RJ nº 211.334

ALINE HERSCOVICI

Pesquisadora em Direito

HELENA SECAF DOS SANTOS

Pesquisadora em Direito