AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.649 DISTRITO FEDERAL

RELATOR	**: MIN. GILMAR MENDES**
REQTE.(S)	: CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL - CFOAB
ADV.(A/S)	: FELIPE DE SANTA CRUZ OLIVEIRA SCALETSKY E OUTRO(A/S)
INTDO.(A/S)	: PRESIDENTE DA REPÚBLICA
PROC.(A/S)(ES)	: ADVOGADO-GERAL DA UNIÃO
AM. CURIAE.	: ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA
ADV.(A/S)	: BRUNO RICARDO BIONI
ADV.(A/S)	: MARIANA MARQUES RIELLI
ADV.(A/S)	: RAFAEL AUGUSTO FERREIRA ZANATTA
ADV.(A/S)	: IZABEL SAENGER NUNEZ
AM. CURIAE.	: LABORATORIO DE POLITICAS PUBLICAS E INTERNET LAPIN
ADV.(A/S)	: JOSE RENATO LARANJEIRA DE PEREIRA
ADV.(A/S)	: PAULO HENRIQUE ATTA SARMENTO
AM. CURIAE.	: INSTITUTO MAIS CIDADANIA
ADV.(A/S)	: LUIZ GUSTAVO DE ANDRADE
ADV.(A/S)	: ROOSEVELT ARRAES

V O T O
(Conjunto ADI 6649 e ADPF 695)

O SENHOR MINISTRO GILMAR MENDES (RELATOR): Trata-se de Ação Direta de Inconstitucionalidade e de Arguição de Descumprimento de Preceito Fundamental que, sob diferentes perspectivas, endereçam a controvérsia relativa aos limites, ao âmbito de proteção e à dimensão axiológica dos direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade, especificamente no que diz respeito ao tratamento de dados pessoais pelo Estado brasileiro.

Inicialmente, saúdo as sustentações orais que antecederam o debate da causa, todas fundadas em substanciosos argumentos de índole

constitucional e em um profundo diálogo com os precedentes desta Corte. Registro que a verticalidade das manifestações e as diferentes concepções que existem sobre a matéria apenas comprovam a indiscutível necessidade de submeter a controvérsia ao escrutínio do Tribunal Pleno.

Não há dúvidas quanto ao assento constitucional da matéria ventilada nas ações de controle concentrado. É o que se conclui por meio de rápida incursão na jurisprudência do Supremo Tribunal Federal, que, ao ser provocado, não se eximiu de enfrentar, em mais de uma ocasião, a constitucionalidade de atos de coleta, armazenamento, transferência e divulgação de dados pessoais por agentes públicos.

Faço referência, pela relevância do precedente, ao memorável julgamento da **Ação Direta de Inconstitucionalidade 6.387**, de relatoria da **EMINENTE MINISTRA ROSA WEBER**, em que o Supremo Tribunal Federal reconheceu a existência de um **direito fundamental autônomo** à proteção de dados pessoais na ordem jurídico-constitucional brasileira. A decisão é importante por diversos aspectos.

Primeiro, por contribuir para a construção de uma dogmática constitucionalmente adequada para o que se tem chamado de era digital, berço de uma sociedade fundada no desenvolvimento tecnológico e no intercâmbio de informações digitais. Segundo, pela enunciação dos vetores interpretativos e do substrato axiológico que devem orientar a compreensão e a aplicação de toda a legislação existente sobre o tema.

Aqui também, nos casos ora em julgamento, surge outra auspiciosa oportunidade para que a Corte, no contexto das relações entre os gestores públicos e os titulares de dados pessoais, examine o âmbito de proteção do direito à autodeterminação informativa**,** mais precisamente os limites e as salvaguardas institucionais que se aplicam ao compartilhamento de informações entre órgãos e entidades da administração pública federal.

Pois bem. Examino inicialmente as preliminares ao mérito suscitadas pela Advocacia-Geral da União na Ação Direta de Inconstitucionalidade 6.649 e na Arguição de Descumprimento de Preceito Fundamental 695.

Em seguida, adentro a controvérsia constitucional que compõe a essência das ações de controle concentrado, debruçando-me sobre as teses

deduzidas pelo Conselho Federal da Ordem dos Advogados do Brasil e pelo Partido Socialista Brasileiro (PSB).

Ao apreciar as ações de controle concentrado, avalio se é legítimo o compartilhamento de dados pessoais entre órgãos e entidades da administração pública federal, examinando a compatibilidade do Decreto 10.046/2019 com o regime de proteção de dados estabelecido pela ordem constitucional brasileira.

I - Admissibilidade

Em manifestação escrita na ADI 6.649, a Advocacia-Geral da União alega o não cabimento da ação direta de inconstitucionalidade para impugnação de regulamentos ou atos normativos que exorbitam do poder regulamentar. Afirma, em síntese, que o Decreto 10.046/2019 constitui ato normativo estritamente subordinado, dependente de lei, de modo que as teses deduzidas pelo autor não caracterizariam ofensa direta ao texto constitucional.

Com a devida vênia, entendo que não prospera a preliminar articulada na manifestação da AGU, pelas razões que passo a expor.

A propósito do tema, a jurisprudência do Supremo Tribunal Federal realmente se consolidou no sentido de não se admitir ação de controle concentrado de atos normativos secundários, quando as razões que inspiram a ação direta pressupõem prévio confronto entre o regulamento administrativo e a legislação infraconstitucional. A esse respeito, são ricas as considerações feitas pelo eminente Ministro Celso de Mello, na **ADI 1.347/DF**:

> [...] o eventual extravasamento, pelo ato regulamentar, dos limites a que se acha materialmente vinculado poderá configurar insubordinação administrativa aos comandos da lei. Mesmo que desse vício jurídico resulte, **num desdobramento ulterior**, potencial violação da Carta Magna, ainda assim estar-se-ia em face de uma situação de **inconstitucionalidade**

> **meramente reflexa ou oblíqua**, cuja apreciação não se revela possível em sede de jurisdição concentrada.

As razões que inspiram essa orientação jurisprudencial são evidentes. Prevalece na doutrina que controlar a constitucionalidade significa aferir a compatibilidade de determinada interpretação ou aplicação de leis ou atos normativos em face do texto constitucional. Como anota **Jorge Miranda**, a constitucionalidade e a inconstitucionalidade designam conceitos de relação, isto é, "*a relação que se estabelece entre uma coisa – a Constituição – e outra coisa – um comportamento – que lhe está ou não conforme, que com ela é ou não compatível, que cabe ou não no seu sentido*" (**Manual de Direito Constitucional**, Coimbra: Coimbra Editora, 1983, pp. 273-274).

São justamente essas premissas que orientaram a jurisprudência do Supremo Tribunal Federal acerca do não cabimento do controle abstrato, quando a articulação da tese de inconstitucionalidade pressupõe prévio exame de dispositivos infraconstitucionais. Por isso, a Corte tem repelido ações diretas fundadas exclusivamente na alegação de insubordinação do *poder regulamentar* aos comandos da lei, nelas identificando uma situação de ofensa meramente reflexa ou oblíqua que escapa dos limites do controle concentrado de constitucionalidade.

Por outro lado, não são poucos, tampouco isolados, os precedentes em que o Tribunal conheceu de ações diretas de inconstitucionalidade ajuizadas contra decretos editados pelo Poder Executivo, sobretudo quando se trata de regulamento com perfil autônomo ou de decreto que, a pretexto de dar fiel execução à lei, exorbita flagrantemente do âmbito do poder regulamentar (**ADI-MC 2.155/PR**, Rel. Min. Sydney Sanches, DJ 1º.6.2001; **ADI-MC 1.435/DF**, Rel. Min. Francisco Rezek, DJ 6.8.1999; **ADI 1.969-MC**, Rel. Min. Marco Aurélio, DJ 5.3.04; e **ADI 2.950-AgR**, Rel. Min. Marco Aurélio, redator para acórdão Min. Eros Grau).

No presente caso, é evidente que o decreto editado pelo Poder Executivo **não se esgota** na mera regulamentação de dispositivos da Lei 12.527/2011, que dispõe sobre o acesso à informação na administração pública, e da Lei 13.709/2018, conhecida como Lei Geral de Proteção de

Dados Pessoais.

Em diversos aspectos, o Decreto 10.046/2019 parece ter força normativa própria, introduzindo alterações na ordem jurídica vigente. É o que ocorre, à guisa de exemplo, com a instituição do Cadastro Base do Cidadão, que reúne, em uma base unificada, informações biográficas que constam nas diferentes *bases temáticas* que atualmente compõem o acervo de dados da Administração Pública Federal (art. 16). Chama a atenção, ainda, a criação do Comitê Central de Governança de Dados (art. 21), com poder de (i) deliberar sobre a exata extensão dos dados biográficos que constarão do Cadastro Base do Cidadão (incisos VII e VIII); (ii) definir as hipóteses de compartilhamento amplo, restrito e específico; e (iii) fixar regras e parâmetros para o compartilhamento de dados entre órgãos da Administração Pública Federal (incisos I e II).

Convém ressaltar que o próprio Presidente da República reconheceu que, ao editar o Decreto 10.046/2019, operava com relativa margem de liberdade, e não apenas com a finalidade de dar fiel execução às leis. Não por outra razão, invocou tanto a prerrogativa prevista no art. 84, *caput*, IV, da Constituição Federal quanto aquela prevista no inciso VI, alínea "a", do mesmo dispositivo, que assegura ao Chefe do Poder Executivo o poder de expedir decretos de perfil não regulamentar, cujo fundamento de validade repousa diretamente na Constituição.

Examino as preliminares suscitadas pela Advocacia-Geral da União na ADPF 695, designadamente as alegações de ausência de indicação precisa do ato do Poder Público, de inobservância do requisito de subsidiariedade e de ausência do interesse de agir.

De início, reputo que a lesão a preceitos fundamentais por ato do Poder Público – compartilhamento de dados da Carteira Nacional de Habilitação entre o SERPRO e a ABIN – parece estar suficientemente indicada na peça inicial, sendo comprovada pelos documentos colacionados aos autos, que indicam (i) a transmissão da informação por veículo de mídia; e (ii) a confirmação desta em manifestação das autoridades. Em um primeiro juízo, tais documentos mostram-se suficientes para a comprovação do ato concreto, em consonância ao art.

3º, II, da Lei 9.882/99.

No mais, intimada, a União juntou aos autos acervo probatório complementar – em especial a Portaria 15/2016, do DENATRAN, e o Termo de Autorização 07/2020, emitido pelo DENATRAN em favor da ABIN, documentos que contribuem para a compreensão dos exatos contornos do ato do Poder Público impugnado na ADPF.

Afasto, ainda, a alegação de ausência de impugnação adequada de todo o complexo normativo em que a medida administrativa está inserida. Dos documentos já ressaltados e dos fundamentos da exordial é possível aferir com perfeição tanto os parâmetros de controle quanto o ato do Poder Público impugnado pelo requerente, sendo isso suficiente ao conhecimento da ADPF.

Também não vislumbro desrespeito ao requisito da subsidiariedade. Importa destacar, a princípio, que a Lei 9.882/99 impõe que a arguição de descumprimento de preceito fundamental somente será admitida se não houver outro meio eficaz de sanar a lesividade (art. 4º, § 1º).

Uma leitura apressada do dispositivo poderia conduzir à compreensão de que o cabimento da arguição de descumprimento de preceito fundamental se restringe às hipóteses de absoluta inexistência de qualquer outro meio capaz de tutelar a ordem constitucional.

Uma leitura mais cuidadosa, porém, revela que, na análise sobre a eficácia da proteção de preceito fundamental, deve predominar enfoque objetivo ou de proteção da ordem constitucional objetiva. Em outros termos, o princípio da subsidiariedade – inexistência de outro meio eficaz de sanar a lesão – há de ser compreendido no contexto da ordem constitucional global.

O caráter enfaticamente objetivo do instituto, assim, enseja a interpretação no sentido de que o meio eficaz de sanar a lesão parece ser aquele apto a solver a controvérsia constitucional relevante de forma ampla, geral e imediata.

No âmbito da ADPF, o ajuizamento da ação e sua admissão estão vinculados, muito provavelmente, ao significado da solução da controvérsia para o ordenamento constitucional objetivo, e não à proteção

judicial efetiva de uma situação singular. Assim, o juízo de subsidiariedade há de ter em vista, especialmente, a lógica já consolidada dos processos objetivos no sistema constitucional (**ADPF 33**, de minha Relatoria; **ADPF 79**, Rel. Min. Cezar Peluso, 4.8.2005; **ADPF 99**, Rel. Min. Ricardo Lewandowski, 8.3.2010; e **ADPF 76**, da minha relatoria, 13.2.2006).

Ante a inexistência de outro processo de índole objetiva apto a solver, de uma vez por todas, a controvérsia constitucional, afigura-se integralmente aplicável a arguição de descumprimento de preceito fundamental. É que as ações originárias e o próprio recurso extraordinário não parecem, as mais das vezes, capazes de resolver a controvérsia constitucional de forma **geral, definitiva e imediata**.

No presente caso, a potencial lesão a preceitos fundamentais consuma-se tão logo ocorra o compartilhamento de dados pessoais pretendido pelas autoridades do Poder Público. Dessa forma, mesmo que fosse cabível o manejo de instrumentos processuais ordinários, não haveria tempo hábil para uma resposta jurisdicional apta a sanar, de modo eficaz, o risco de grave comprometimento de valores essenciais contemplados pelo texto constitucional.

Rememoro também a fórmula da **relevância do interesse público** para justificar a admissão da arguição de descumprimento – explícita no modelo alemão –, que está implícita no sistema criado pelo legislador brasileiro, tendo em vista o caráter marcadamente objetivo que conferiu ao instituto.

Assim, o Supremo Tribunal Federal poderá, ao lado de outros requisitos de admissibilidade, emitir juízo sobre a relevância e o interesse público contido na controvérsia constitucional, podendo recusar a admissibilidade da ADPF sempre que não vislumbrar relevância jurídica na sua propositura.

O caso concreto tem a necessária relevância. Tem por fim evitar a lesão ao direito fundamental à dignidade da pessoa humana, à intimidade e à vida privada, na esteira do reconhecimento, em julgamento recente do Tribunal Pleno, da proteção de dados pessoais

como direito fundamental autônomo (**ADI 6.387**, Rel. Min. Rosa Weber).

Enfim, por qualquer ângulo que se aprecie a matéria, não me parece razoável impedir o escrutínio do tema pelo Supremo Tribunal Federal, seja pela relevância das teses invocadas na ADPF, que se relacionam diretamente com o regime constitucional de proteção de dados pessoais, seja pelo risco de afetação da privacidade de milhares de brasileiros.

O presente julgamento franqueia ao Tribunal Pleno a possibilidade de se debruçar sobre o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público. Põe em perspectiva, portanto, uma questão de crucial importância para qualquer sociedade democrática contemporânea, qual seja, o alcance, os limites e a fisionomia do direito à autodeterminação informativa.

Assim, com a devida vênia, entendo que seria temerário subtrair essa questão do controle abstrato de normas pelo Supremo Tribunal Federal, relegando-a a instrumentos processuais que não oferecem meios de solver a controvérsia constitucional de forma ampla, geral e imediata.

Por tudo, a arguição de descumprimento de preceito fundamental não apresenta óbices intransponíveis a impedir a apreciação das teses articuladas na inicial (art. 4º da Lei 9.882/1999).

II – Mérito

Não há como negar que existem razões fundadas para as preocupações externadas pelo requerente. Infelizmente, ainda há autoridades públicas que insistem no mau vezo de inverter a hierarquia das normas, acreditando menos na Constituição e nas leis do que em regulamentos editados pelo Poder Executivo. E, o que é pior, não raras vezes essa postura se ampara em leituras distorcidas do próprio texto do ato regulamentar, cujos limites semânticos não dão margem para a interpretação ilegítima proposta pelo administrador (também comum, nessa seara, é a tentação de fraudar a jurisdição deste Supremo Tribunal Federal mediante o achamboado expediente de revogações de atos

infralegais às vésperas de sessão de julgamento).

Os exemplos são os mais variados e falam por si. Sem grandes digressões, temos aqui, em julgamento na ADPF 695, uma tentativa obscura de compartilhamento massivo dos dados pessoais de 76 milhões de brasileiros com órgãos integrantes do Sistema Brasileiro de Inteligência. Causa perplexidade que, ao se manifestar nos autos, a União pretendeu amparar essa prática manifestamente inconstitucional em permissões supostamente conferidas pelo Decreto 10.046/2019, ignorando os princípios mais comezinhos do regime constitucional de proteção de dados.

Além disso, todos nós conhecemos – porque a controvérsia desaguou neste Tribunal – a tentativa de edição da Medida Provisória 954/2020, que determinava que as operadoras de telefonia disponibilizassem ao IBGE, em meio eletrônico, os nomes, números de telefone e endereços de milhões de usuários de serviços de telecomunicação. O caso foi conduzido com excelência pela **EMINENTE MINISTRA ROSA WEBER,** que não hesitou em apontar a flagrante inconstitucionalidade da medida provisória e o risco que ela oferecia a liberdades públicas consagradas pelo regime democrático (**ADI 6.387**).

Também é grave a notícia trazida pelo *Laboratório de Políticas Públicas e Internet* de que o Comitê Central de Governança de Dados, no exercício de suas atribuições regulamentares, **recomendou** que **dados pessoais** fossem submetidos ao nível de compartilhamento restrito**.** Segundo cartilha elaborada pelo Comitê, pertenceriam a essa categoria as seguintes informações biográficas: nome completo, endereço, números de identificação (CPF, NIS e título eleitoral), situação civil, data de nascimento, telefone e endereço de *email* (disponível em https://www.gov.br/governodigital/pt-br/governanca-de-dados/formulario_regras-de-compartilhamento_modelo-v1-0.pdf).

O evento preocupa, na medida em que, por definição, o nível de compartilhamento restrito engloba dados que, apesar de sigilosos, podem ser livremente acessados **por todos** os órgãos e entidades da Administração Pública Federal. Cuida-se, assim, de categoria que almeja

impedir o acesso do **público externo** a dados cujo sigilo seja imprescindível à segurança da sociedade e do Estado, sem obstaculizar o **livre fluxo** das informações entre os diferentes órgãos que compõem o aparelho estatal.

Por permitirem ampla difusão de dados sensíveis entre entidades governamentais, os limites impostos pelo nível de compartilhamento restrito oferecem proteção inadequada para a tutela dos valores estruturantes da LGPD. **Salta aos olhos, portanto, o manifesto equívoco cometido pelo Comitê Central de Governança de Dados, ao editar recomendação que encerra grave risco de malversação de dados pessoais e de violação da privacidade dos usuários do serviço público**.

Tudo isso reforça a premente necessidade de exercermos com extremo rigor o controle de políticas públicas que possam afetar substancialmente o direito fundamental à proteção de dados pessoais. **No caso específico do Decreto 10.046/2019, diante dos excessos praticados pela Administração Pública Federal, impõe-se uma correção de rumos, com o objetivo de imunizar o texto normativo contra leituras desviantes da Constituição Federal**.

Para tanto, afigura-se adequada solução que, preservando ao máximo a autoridade do Chefe do Poder Executivo e o espaço de conformação que é inerente ao exercício do poder regulamentar, empreenda **interpretação do Decreto 10.046/2019 que o coloque em conformidade com a Constituição Federal**.

Nessa senda, cumpre que indaguemos, antes de mais nada, se a interpretação conforme à Constituição tem lugar para o caso em apreço. A resposta para tanto passa pela devida contextualização da interpretação conforme à Constituição no quadro mais geral das **fórmulas decisórias intermediárias**.

A expansão de tarefas e papéis atribuídos ao poder público, mormente após a segunda metade do século XX, importou em novo modelo de organização política, o "Estado Social", cuja realização dependia de um incremento (tanto no campo temático como no grau de intensidade) das atividades legislativa e administrativa. (FORSTHOFF,

Ernst. "Begriff und Wesen des sozialen Rechtsstaates". In: **Rechtsstaat im Wandel. Verfassungsrechtliche Abhandlungen, 1950-1964**. Stuttgart: W. Kohlhammer, 1964, p. 38; ALEXY, Robert. **Theorie der Grundrechte**. Frankfurt: Suhrkamp, 1986, p. 395 e ss.).

Ao Estado foram imputados deveres até então inéditos e, de seu descumprimento, originaram-se **expedientes inconstitucionais também singulares**, frente aos quais a jurisdição constitucional teve que aprender a lidar. Tal como a chamada **omissão parcial**. Nela, como leciona Hartmut Maurer, a inconstitucionalidade se materializa em uma **disciplina normativa diferenciada** (*Unterschiedlichkeit der Regelung*), que vulnera o **princípio da isonomia.** (MAURER, Hartmut. "Zur Verfassungswidrigerklärung von Gesetzen". In: **Im Dienst an Recht und Staat: Festschrift fur Werner Weber**. Berlim: Dunker und Humbolt, 1974, p. 345).

Assim, diz Jörn Ipsen, a inconstitucionalidade não é imputável a uma regra jurídica isoladamente considerada: o que se tem é a **inconstitucionalidade de uma chamada relação normativa** (*verfassungwidrige Normrelation*) (IPSEN, Jörn. **Rechtsfolgen der Verfassungsidrigkeit von Norm und Eizelakt**. Baden-Baden: Nomos Verlag, 1980, p. 213 e ss.)

Nesse sentido, o **Tribunal Constitucional Alemão,** já em 1958, no caso *Teuerungszulage*, lavrou ensinamento jurisprudencial destinado a fazer fortuna no constitucionalismo contemporâneo: em se tratando de **omissão parcial,** não obstante a inconstitucionalidade da norma, uma consequente declaração de nulidade "***causaria uma situação na qual a ordem constitucional seria respeitada ainda menos***". (BVerfGE 8, 1, Primeiro Senado, em 11 de junho de 1958).

O tratamento dogmático e jurisprudencial da omissão parcial foi apenas o primeiro passo. Desde então, **os tribunais constitucionais desenvolveram amplo leque de fórmulas decisórias intermediárias**, expressão pela qual Gustavo Zagrebelsky e Valeria Marcenò agrupam estilos de **decisões** e **técnicas** processuais cujo traço comum está em conferir, à jurisdição constitucional, possibilidades outras que não o

binário "lei constitucional e portanto válida" *versus* "lei inconstitucional e portanto nula". Técnicas essas funcionalmente orientadas para preservar a utilidade das decisões dos Tribunais Constitucionais naqueles casos em que – pontifica Zagrebelsky – "*a eliminação pura e simples da lei não remediaria a inconstitucionalidade, mas concorreria, paradoxalmente, a* ***produzir resultados de inconstitucionalidade ainda mais grave***". (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria. **Giustizia Costituzionale**. Bolonha: il Mulino, 2012, p. 338).

A **interpretação conforme à Constituição** insere-se plenamente nesse marco. Filia-se ao gênero das **técnicas decisórias intermediárias**, porquanto seu uso pressupõe e orienta-se pela **função primordial de afastar a produção de resultados inconstitucionais**. Para assim fazê-lo, a interpretação conforme à Constituição se vale da diferença entre **texto** e **norma**, nisso compreendidas distinções correlatas, como **disposição** e **norma, texto legislativo** e **programa normativo** etc. **Pressuposto hermenêutico** este que, de resto, fundamenta técnicas decisórias intermediárias congêneres, como a declaração parcial qualitativa de inconstitucionalidade.

É em conformidade com esses pressupostos que a técnica da interpretação conforme consegue evitar a solução radical de operar o expurgo total ou parcial de texto normativo. Trata-se de solução que observa aquela "**exigência de gradualidade**" que se espera das intervenções de um Tribunal quando em jogo atos normativos produzidos pelos demais Poderes.

Daí o acerto de Zagrebelsky ao pontificar que "*a inconstitucionalidade da lei é a falência da interpretação*". Sim, porque a adoção de "**soluções menos incidentes**", como a interpretação conforme e demais técnicas intermediárias, não é algo desejável apenas por motivos de ordem prática, e sim postura que se espera do julgador por **razões de ordem constitucional** (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria. **Giustizia Costituzionale**. Bolonha: il Mulino, 2012, p. 385 e 401). Razões como a cláusula da **separação dos poderes** e demais princípios que a desenvolve, como o **princípio da conformidade funcional** (MENDES,

Gilmar Ferreira. BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional.** 14ª ed. São Paulo: Saraiva, 2019, p. 94).

Nesse marco, deixo expressamente assentado que o **primeiro critério** que servirá de norte para o manejo da **interpretação conforme à Constituição** no caso em apreço, é aquele que homenageia a **função** precípua dessa técnica de decisão intermediária: a de **afastar a produção de resultados inconstitucionais extremos**.

Explicito, também, um **segundo critério**.

É bem verdade que é mais simples divisar uma **dimensão negativa** da interpretação conforme à Constituição. Assim se dá quando, por exemplo, o Tribunal delibera pela exclusão de interpretações consideradas inconstitucionais. Mas nem só de efeitos cassatórios vive a interpretação conforme à Constituição. As Cortes Constitucionais também se valem dessa técnica para **colmatar lacunas**, em **atividade de otimização constitucional**, mediante a qual, preleciona Christoph Gusy, se procede à construção normativa por **analogia**, **redução**, ou por **derivação** de premissas normativas da Constituição (GUSY, Christoph. **Parlamentarischer Gesetzgeber und Bundesverfassungsgericht**. Berlim: Duncker und Humblot, 1985, p. 214; ZIPPELIUS, Reinhold. "Verfassungskonform Auslegung von Gesetzen". In: **Bundesverfassungsgericht und Grundgesetz**. Vol. 2. Tübingen: Mohr Siebeck, 1976, p. 121).

É assim porque, há tempos, a atuação da jurisdição constitucional não mais se resume àquela **função negativa**, relacionada à eliminação de normas contrárias à Constituição descrita pela figura do "legislador negativo". Desempenha também **funções positivas** de "**recomposição interpretativa**" e de "**integração normativa**" do ordenamento jurídico. (ZAGREBELSKY, Gustavo e MARCENÒ, Valeria. **Giustizia Costituzionale**. Bolonha: il Mulino, 2012, p. 338).

Coerente a esse marco, o Professor Emérito da Universidade de Roma "La Sapienza" e Juiz da Corte Constitucional da Itália, Franco Modugno, ensina que da interpretação conforme à Constituição não se espera, apenas, a função negativa de invalidação de normas oriundas da

interpretação de um dispositivo, mas também a **função positiva** de promover a coerência do ordenamento jurídico, obstando que a legislação infraconstitucional faça "sistema em si mesma", no exato instante em que promove a integração desta com o plexo normativo superior. (MODUGNO, Franco. "Metodi ermeneutici e Diritto Costituzionale". In: **Scritti sull'Interpretazione Costituzionale**. Nápoles: Editoriale Scientifica, 2008, p. 68 e ss.)

Não poderia ser diferente, uma vez que a interpretação conforme à Constituição traduz espécie, variante ou subdivisão da **interpretação sistemática** (SPANNER, Hans. "Die verfassungskonforme Auslegung in der Rechtsprechung des Bundesverfassungsgerichts". In: **Archiv des öffentlichen Rechts**. Vol. 91, n. 4. Tübingen: Mohr Siebeck, 1966, p. 503; HAAK, Volker. **Normenkontrolle und verfassungskonforme Gesetzesauslegung des Richters**. **Eine rechtsvergleichende Untesuchung.** Bonn: Roehrscheid, 1963, p. 259; EBSEN, Ingwer. **Das Bundesverfassungsgericht als Element gesellschaftlicher Selbstregulierung. Eine pluralistische Theorie der Verfassungsgerichtsbarkeit im demokratischen Verfassungsstaat**. Berlim: Duncker und Humblot, 1985, p. 91).

Precisamente por isso, a interpretação que busque garantir a supremacia da Constituição requer que a superioridade da norma constitucional ocorra não apenas **negativamente**. A Constituição não pode ser reduzida à função de fornecer um limite ao direito infraconstitucional, exatamente porque o texto maior é algo que se realiza no tempo, e não um dado inerte:

> "Não é um dado 'inerte' que possa ser tomado como critério fixo para determinar um ponto exato dentro de uma banda de oscilação de significados normativos possíveis de uma disposição legislativa. Em outras palavras, interpretar uma disposição com base em outras significa realizar uma interpretação sistemática, **isto é, construir uma norma compatível com todas**." (CHESSA, Omar. "Non manifesta infondatezza *versus* interpretazione adeguatrice?". In:

> D'AMICO, Marilisa; RANDAZZO, Barbara (orgs.). **Interpretatzione conforme e tecniche argomentative**. Turim: Ed. Giappichelli, 2009, p. 272) (grifou-se).

Daí ser premente a valorização do componente **positivo** da superioridade da Constituição, que conduz à transformação dos dispositivos interpretados em normas consoantes à Constituição. Exsurge, com isso, o **segundo critério** que orientará o uso da técnica decisória requerida: uma interpretação adequada das normas infralegais ora impugnadas não há de se contentar com o simples cotejo da literalidade do texto de decretos com padrões normativos superiores (Lei Geral de Proteção de Dados, Constituição Federal). Antes, **exige reconstrução normativa sistemática**.

Atento a essas premissas, assinalo que, no caso vertente, a declaração de inconstitucionalidade de todo o panorama normativo, esvaziando todo o seu alcance, acabaria por destituir os órgãos do Poder Executivo de normas operacionais necessárias ao compartilhamento de dados no interesse da eficiente prestação de serviços públicos. Nesse sentido, a extirpação pura e simples da norma impugnada poderia acarretar, fundamentalmente, a formação de vácuo regulamentar numa área relevante e sensível para o gestor público, com impactos nocivos para a eficiência e segurança da atividade administrativa.

Em um outro cenário, caso se entenda pela **repristinação** do Decreto 8.789/2016, revogado pelo atual regulamento, **o resultado seria ainda mais nocivo à proteção de privacidade**. A norma anterior estabelecia que os dados cadastrais sob gestão dos órgãos públicos federais seriam "***compartilhados*** *entre as bases de dados oficiais,* ***preferencialmente de forma automática****, para evitar novas exigências de apresentação de documentos e informações e possibilitar a atualização permanente e simultânea dos dados*".

Dado o obsoletismo do texto anterior, é lícito concluir que o efeito repristinatório da declaração de inconstitucionalidade causaria ainda mais insegurança e instabilidade, na medida em que os dispositivos revogados não apenas impunham o compartilhamento **automático** de informações cadastrais entre todos os órgãos públicos federais, como

também **silenciavam completamente a respeito da adoção de salvaguardas institucionais para proteção de dados pessoais.**

Evidencia-se, a não mais poder, a necessidade de adoção da técnica decisória intermediária da interpretação conforme à Constituição.

Com efeito, por qualquer ângulo que se observe a matéria, parece-me mais adequado, no contexto do equilíbrio que deve existir entre os Poderes, preservar o programa normativo contido no decreto presidencial em tudo aquilo que estiver alinhado com a Constituição Federal. E, como visto, são muitas as possibilidades de tratamento legítimo de dados pessoais por órgãos e entidades governamentais.

Por tudo o quanto foi dito, adianto que o objeto desta fiscalização em abstrato de constitucionalidade, o Decreto 10.046/2019, pode ostentar sentido compatível com o texto constitucional. Ante a polissemia da norma, que conduziu a eventos recentes de grave descumprimento de preceitos fundamentais, é dever do Tribunal atuar diligentemente para, empregando a técnica decisória adequada, subtrair do campo semântico da norma eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais.

Passo a fazê-lo, atento, em primeiro lugar, ao papel que a jurisdição constitucional tem assumido, no direito comparado, para a criação de mecanismos de salvaguarda de posições jurídico-fundamentais em face do desenvolvimento tecnológico. Após, discorro sobre o âmbito de proteção e perfil do direito fundamental em jogo (autodeterminação informacional), bem como sua concorrência com princípios formais como o da supremacia do interesse público. Realizado esse percurso, obteremos o parâmetro adequado, acredito, para conformar o programa normativo do Decreto 10.046/2019 à Constituição Federal.

2.1 – Inovação jurídica como contraface da inovação técnica: a permanente abertura da ordem constitucional à transformação tecnológica por obra da jurisdição constitucional comparada.

A discussão travada nestes autos testa as possibilidades e os limites

da proteção constitucional do direito à privacidade (art. 5º, inciso X, da CF), *vis-à-vis* os riscos desencadeados pelo constante avanço tecnológico que caracteriza a nossa sociedade da informação.

Na era digital, as novas tecnologias de comunicação se tornaram condição necessária para a realização de direitos básicos – como se faz evidente no campo da liberdade de expressão, de manifestação política e de liberdade religiosa. Contudo, verifica-se que esses mesmos avanços tecnológicos suscitam riscos generalizados de violação de direitos fundamentais básicos.

Como muito bem destacado por **Wolfgang Hoffmann-Riem**, é necessário que, diante das ameaças geradas pelo desenvolvimento da tecnologia, a jurisdição constitucional atue como instrumento de inovação jurídica, visando à constante atualização da tutela dos direitos fundamentais:

> As tecnologias oferecem um enorme potencial, e não é exagero referir-se às oportunidades decorrentes da sociedade da informação. **Na maioria dos aspectos da vida diária, os cidadãos são hoje obrigados a utilizar as novas tecnologias para não serem social e economicamente marginalizados**. Mas as novas tecnologias também trazem consigo um potencial de perigo: não só o de terceiros, incluindo o Estado, penetrando na esfera privada, mas também o desenvolvimento de um poder de comunicação e de poder econômico que impõe seus interesses seletivamente através de manipulação ou por outros meios (tradução livre) (HOFFMANN-RIEM, Wolfgang. "Innovaciones en La Jurisprudencia del Tribunal Constitucional Alemán, a Propósito de la Garantía De Los Derechos Fundamentales En Respuesta A Los Cambios Que Conducen A La Sociedad De La Información". In: **ReDCE**, n. 22, 2014).

O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. O crescimento exponencial das atividades de coleta, tratamento e análise de dados pessoais possibilita que governos e

empresas utilizem algoritmos e ferramentas de *data analytics*, promovendo classificações e esteriotipações discriminatórias de grupos sociais na tomada de decisões estratégicas para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.

Alguns exemplos nesse sentido são dignos de nota. Nos Estados Unidos, por exemplo, uma ferramenta de gerenciamento automatizado do sistema prisional chamada de *Correctional Offender Management Profiling for Alternative Sanctions* (COMPAS) tem sido utilizada para avaliação do risco de reincidência dos egressos. Essa ferramenta funciona a partir de árvore decisória, que classifica os detentos em um espectro de risco que varia de um a nove, sendo nove o mais alto e um o mais baixo.

Em 2017, a Suprema Corte de Wisconsin manteve a condenação de um réu que foi acusado de fugir da polícia ao dirigir um carro anteriormente utilizado em um tiroteio. Ele havia sido condenado previamente por agressão sexual e, após uma avaliação do algoritmo, considerou-se que havia alto risco de reiteração delitiva, a justificar a imposição da pena privativa de liberdade de seis anos.

Todo esse panorama nos indica que, em certas áreas, o processo artesanal de tomada de decisões críticas para o Estado de Direito tem sido progressivamente substituído por soluções automatizadas. Em decorrência dessas transformações, é inequívoco que, sob o influxo da dimensão objetiva dos direitos fundamentais, surge um dever estatal de proteção dos valores estruturantes do regime democrático, por meio da criação de salvaguardas institucionais que preservem a essência da cidadania.

É por isso que, diante dos riscos inerentes à sociedade da informação, **cabe ao Tribunal, de um lado, reconhecer que a disciplina jurídica do processamento e da utilização de dados pessoais acaba por afetar o sistema de proteção de garantias individuais como um todo e, de outro, proceder a uma releitura de mecanismos clássicos de defesa**

das liberdades públicas e do Estado Democrático de Direito.

Esse ambiente faz com que os Tribunais Constitucionais tenham que proceder a uma constante reafirmação da força normativa da Constituição, de modo a preservar garantias individuais que constituem a base do regime democrático e que, hoje, são diretamente ameaçadas pelo descompasso entre o poder de vigilância e os mecanismos de proteção da intimidade.

Os riscos inerentes à era digital devem ser considerados na leitura e na aplicação da Constituição Federal de 1988. Aliás, ousaria dizer que **nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica**. Dentro da tradição do *judicial review* norte-americano, por exemplo, mesmo os juristas partidários do *originalismo constitucional* reconhecem que a inovação naturalmente levanta questões sobre como a Constituição se aplica aos novos fenômenos sociais. Como advertiu o professor Lawrance Lessig, em 1996, no contexto da disseminação da internet:

> "Os *Founding Fathers* deram ao povo uma Constituição para um mundo onde a tecnologia era imperfeita. Nesse mundo, a liberdade reinava, não tanto porque a lei positiva a criava; mas porque as tecnologias imperfeitas se submetiam à justiça. Quando as tecnologias daquele mundo mudam, nós nos confrontamos com uma escolha. **Podemos permitir que a ideia de eficiência tecnológica impere nesse novo espaço digital, fazendo com que as liberdades protegidas pela Constituição se esvaziem; ou podemos recriar as esferas de liberdade para superar àquelas pensadas em um contexto de imperfeição tecnológica**" (tradução livre) (LESSIG, Lawrence. "Reading The Constitution in Cyberspace". In: **Emory Law Review**, v. 45, p. 869–910, 1996, p. 41).

Essa visão, a propósito, foi muito bem simbolizada no voto dissidente do **Juiz Louis Brandeis,** em 1928, no caso *United States v. Olmstead.* O processo envolvia discussão acerca do alcance normativo da

Quarta Emenda da Constituição norte-americana, que garante a inviolabilidade da pessoa, da sua casa, de seus documentos e de seus bens contra a realização de buscas e apreensões ilegítimas (*unreasonable searches and seizures*). Havia dúvida sobre a incidência dessa garantia no caso de interceptação telefônica realizada por meio da instalação de equipamento de escuta em cabos telefônicos localizados na via pública. O **voto majoritário** considerou que, como ouvir uma conversa telefônica privada não exige invasão física do espaço privado do cidadão – o interior da residência –, não seria necessária a prévia autorização judicial.

A **divergência** inaugurada pelo Juiz Brandeis, por outro lado, reconheceu o caráter fundamental do direito à privacidade, encarado por ele como pedra angular do regime de liberdades assegurado pela Constituição americana (*"the most comprehensive of rights and the right most favored by civilized men"*). Partindo dessa premissa, sustentou que, mesmo nos casos em que não ocorre a invasão do domicílio, a realização de interceptação telefônica dependeria de prévia autorização judicial.

Entre os fundamentos de seu voto, o Juiz da Suprema Corte reconheceu a necessidade de **conferir às garantias constitucionais uma capacidade de adaptação aos novos fenômenos sociais**. Alertou ainda que:

> "(...) *assim como as limitações gerais aos poderes de governo, como as incorporadas na cláusula do devido processo legal, não podem proibir o Estado de legislar sobre fenômenos modernos que um século atrás, ou mesmo meio século atrás, provavelmente seriam considerados arbitrários, (...) da mesma forma, as normas jurídicas que garantem ao indivíduo proteção contra abusos de poder específicos também devem ter uma capacidade de adaptação a um mundo em constante mudança*" (tradução livre) (**Olmstead v United States** 277 US 438, 472, 1928, Voto Dissidente do Juiz L. Brandeis).

Essa abertura da jurisdição constitucional à transformação tecnológica enquanto instrumento de preservação dos direitos fundamentais também é consolidada na tradição continental. No icônico

precedente da Lei do Censo alemã, julgado em 1983 (*BVerfGE* 65, 1), cuja análise será aprofundada neste voto, resta evidente que o avanço das técnicas de coleta e processamento de dados foi tomado como válvula de reconfiguração da proteção jurídica à personalidade. A decisão baseou-se principalmente no diagnóstico de que, a partir da coleta e cruzamento de dados do censo, "*seria possível a criação de um quadro abrangente e detalhado da respectiva pessoa - um perfil de personalidade -, mesmo na área íntima; o cidadão torna-se uma verdadeira 'pessoa transparente*"'.

Desse modo, em linha com todas essas experiências históricas, assento que o espírito hermenêutico que deve guiar o Tribunal no tratamento da matéria em exame deve ser o de renovar o compromisso de manter viva a força normativa da Constituição Federal de 1988, nela encontrando caminhos, e não entraves, para a proteção jurídica da intimidade enquanto garantia básica da ordem democrática.

2.2 - Direito fundamental à proteção de dados pessoais: da proteção à intimidade à consagração no texto constitucional (EC n. 115/2022)

Dentro da teoria jurídica moderna, a compreensão histórica do direito à privacidade é comumente vinculada – com todas as possíveis e necessárias ressalvas – à publicação do seminal artigo "*The Right to Privacy*", escrito por **Samuel Warren** e **Louis Brandeis** ainda no final do século XIX (Warren, S., & Brandeis, L. (1890). "The Right to Privacy". **Harvard Law Review**, 4(5), p. 193-220). Esse texto revelou-se paradigmático por ter possibilitado, a partir de precedentes da tradição do *common law*, a identificação de um direito de privacidade de natureza pessoal independente da estrutura da tutela da propriedade.

Nessa concepção tradicional, o direito à privacidade pressupunha uma dicotomia entre as esferas pública e privada, de maneira que o núcleo de sua proteção jurídica se esgotava no direito de ser deixado só ("*the right to be left alone*"). Em sentido fortemente individualista, a proteção atribuída ao direito à privacidade voltar-se-ia, portanto, a

reconhecer uma posição estática e absenteísta do Estado: o direito do titular de retrair aspectos de sua vida do domínio público (BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** São Paulo: Editora Gen, 2019, p. 95).

Entre nós, estudos voltados à identificação da autonomia do Direito à Privacidade parecem ter-se vinculado inicialmente a essa abordagem formal de um direito negativo de não intervenção. Tal abordagem foi reproduzida em artigo clássico do professor **Tércio Sampaio Ferraz Júnior** intitulado "*Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado*", publicado em 1993 (FERRAZ JÚNIOR, Tércio. "Sigilo de dados: o direito à privacidade e os limites da função fiscalizadora do estado". In: **Revista da Faculdade de Direito da Universidade de São Paulo**, v. 88, 1993, p. 430-459).

Como corolário imediato da compreensão do direito à privacidade como uma proteção de caráter essencialmente negativo, eclodiu nos Tribunais brasileiros orientação jurisprudencial restritiva quanto ao âmbito de proteção do art. 5º, inciso XII, da Constituição da República. A título exemplificativo, reporto-me ao entendimento firmado no **RE 418.416**, Rel. Min. Sepúlveda Pertence, DJ de 10.05.2006, em que a Corte referendou o acesso de órgãos policiais a **dados armazenados** em discos rígidos (*hard disks*) apreendidos a partir de busca e apreensão autorizada pelo Poder Judiciário.

Naquela assentada, fazendo expressa referência à fórmula consagrada pelo professor **Tércio Ferraz**, o eminente Ministro Relator assentou que a proteção a que se refere o art. 5º, inciso XII, da Constituição Federal alcançaria apenas a **comunicação** de dados, **e não os dados em si mesmos**. Dessa forma, seria lícita a extração, no interesse da Justiça Criminal, de dados armazenados em equipamentos de informática apreendidos na sede da empresa investigada, desde que, evidentemente, a busca e apreensão tenha sido autorizada pela autoridade judicial competente.

Essa concepção do direito à privacidade como uma garantia individual de abstenção do Estado na esfera privada individual, todavia,

passou por profundas transformações no decorrer do século XX. Devido ao próprio avanço das tecnologias da informação, assistiu-se a uma notória transformação do sentido e do alcance do direito à privacidade. Nas palavras de **Stefano Rodotà** vivenciamos verdadeiro "*processo de inexorável reinvenção da privacidade*" (RODOTÀ, Stefano**. A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008, p. 15).

Tal processo de reinvenção do direito à privacidade é analisado com esmero e profundidade em seminal monografia do professor **Danilo Doneda.** Ao examinar as sucessões geracionais das leis de proteção de dados a partir da década de 1970, bem como o espraiamento da proteção jurídica da privacidade em tratados internacionais ao longo do século XX, o autor assevera que:

> "A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto sua adequação às novas tecnologias da informação. Não basta pensar a privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma 'predileção' individual, associada basicamente ao conforto e comodidade. (...)
>
> Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância: passa a ser um pressuposto para que ela não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada e inviabilizariam o livre desenvolvimento da sua personalidade.
>
> A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento positivo, indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo

> são componentes orgânicos" (grifos nossos) (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Renovar: Rio de Janeiro, 2006, p. 141-142).

A construção de uma nova dogmática constitucional acerca da tutela da privacidade coincide com o reconhecimento, em 1983, do direito à autodeterminação informacional (*die informationelle Selbsstbestimmung*) pelo Tribunal Constitucional Alemão.

A característica especial do direito à autodeterminação informativa não é resultante de um invencionismo episódico, mas sim de "*várias linhas de argumentação da jurisprudência do Tribunal, que já na decisão do microcenso, com recurso à sua jurisprudência sobre a dignidade humana, atribuiu ao cidadão individual uma esfera inviolável da vida privada, da qual se supõe que a influência da autoridade pública deve ser removida*" (FRANZIUS, Claudio. "Das Recht auf informationelle Selbstbestimmung". **Zeitschrift für das juristische Studium.** Gießen, 2015, p. 262).

No paradigmático *Volkszählungsurteil* (*BVerfGE* 65, 1), de 1983, o Tribunal declarou a inconstitucionalidade da chamada Lei do Censo alemã (*Volkszählunsgesetz*), que possibilitava que o Estado realizasse o cruzamento de informações sobre os cidadãos para mensuração estatística da distribuição especial e geográfica da população. Nesse julgado, a Corte Constitucional redefiniu os contornos do direito de proteção de dados pessoais, situando-o como verdadeira projeção de um direito geral de personalidade para além da mera proteção constitucional ao sigilo.

A partir da leitura ampliativa do artigo 2.1, em conjunto com o artigo 1.1. da *Grundgesetz*, o Tribunal Constitucional reconheceu a existência de um direito constitucional de personalidade que teria como objeto de proteção o poder do indivíduo de "decidir sobre a divulgação e o uso dos seus dados pessoais" („*selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen*"), de "decidir sobre quando e dentro de quais limites os fatos da sua vida pessoal podem ser revelados" („*zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden*") e ainda "de ter conhecimento sobre

quem sabe e o que sabe sobre si, quando e em que ocasião" („*wissen können, wer was wann und bei welcher Gelegenheit über sie weiß*"). (FRANZIUS, Claudio. "Das Recht auf informationelle Selbstbestimmung". **Zeitschrift für das juristische Studium.** Gießen, 2015, p. 259).

No caso concreto, o Tribunal entendeu que o processamento automatizado dos dados, possibilitado pela Lei do Censo de 1983, colocaria em risco o poder do indivíduo de decidir por si mesmo sobre se, e como, ele desejaria fornecer seus dados pessoais a terceiros. A situação de risco identificada pelo Tribunal referia-se à possibilidade concreta de, por meio de sistemas automatizados, as informações fornecidas sobre profissões, residências e locais de trabalho dos cidadãos serem processadas de modo a se formar um "perfil completo da personalidade".

Essa nova abordagem 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.

Como bem destacado na decisão, a identificação de um constante avanço tecnológico demanda igualmente a afirmação de um direito de personalidade que integre o contexto das "condições atuais e das futuras circunstâncias do processamento automático de dados" ("*heutigen und künftigen Bedingungen der automatischen Datenverarbeitung*").

É justamente essa reconfiguração que possibilita a afirmação do direito à autodeterminação informacional como contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo. Nas palavras ilustres de **Stefano Rodotà,** a privacidade também passa a ser definida como "o direito de manter o controle sobre suas próprias informações e de determinar como a privacidade é alcançada e, em última instância, como o direito de escolher livremente o seu modo de vida" (tradução livre) (RODOTÀ, Stefano. **In diritto di avere**. Roma: Laterza, 2012, p. 321).

Essa nova abordagem também engloba uma proteção abrangente

que desloca o eixo da proteção de dados para as possibilidades e finalidades de seu processamento. Como bem destacado por **Laura Schertel Mendes**, é decisivo para a concepção do direito à autodeterminação "*o princípio segundo o qual não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados*", 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 de quão sensíveis ou íntimos eles são)*" (**MENDES, Laura Schertel**. "Autodeterminação informativa: a história de um conceito". In: **Revista Pensar**, Vol. 25, n. 4, pp. 1-18, 2020).

A abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pode ser identificada na própria jurisprudência do Supremo Tribunal Federal. Ao apreciar o tema 582 da sistemática da repercussão geral, o Tribunal Pleno reconheceu o direito de acesso do contribuinte a banco de dados da Receita Federal que armazena informações de interesse da arrecadação federal (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, DJe 30.9.2015).

No julgamento, o voto proferido pelo **EMINENTE MINISTRO LUIZ FUX** reforçou o dever qualificado de proteção que é inerente ao armazenamento de informações pessoais em bancos de dados de entidades governamentais ou de caráter público geridos por entidades privadas. Contribuindo decisivamente para a gênese da jurisprudência atual sobre o regime constitucional de proteção de dados, o eminente Relator ressaltou que o art. 1º da Lei 9.507/97, que disciplina o *habeas data*, institui restrições para a divulgação de informações pessoais armazenadas em bancos de dados públicos, limitando "*a divulgação a outros órgãos, que não o detentor das informações, ou a terceiros, que não o titular dos dados registrados*".

Essa evolução jurisprudencial culminou, recentemente, no reconhecimento pelo Tribunal de que a **proteção de dados pessoais** e a **autodeterminação informacional** são direitos fundamentais autônomos, dos quais decorrem **tutela jurídica específica** e **dimensão normativa própria** (**ADI 6.387**, Rel. Min. Rosa Weber). Em eloquente manifestação, o

colegiado afirmou a necessidade de instituição de um controle efetivo e transparente da coleta, armazenamento, aproveitamento, transferência e divulgação de dados pessoais, ao mesmo tempo que reforçou a importância de a Corte exercer com extremo rigor o controle de políticas públicas que possam afetar substancialmente o direito fundamental à proteção de dados.

A partir de leitura abrangente do texto constitucional, especialmente do direito à privacidade e ao livre desenvolvimento da personalidade, o voto da **EMINENTE MINISTRA ROSA WEBER** suspendeu a eficácia da Medida Provisória 954/2020, editada em decorrência da pandemia da COVID-19, que determinava que as operadoras de telefonia disponibilizassem ao IBGE, em meio eletrônico, os nomes, números de telefone e endereços de milhões de usuários de serviços de telecomunicação.

Na ocasião, o Tribunal assentou três balizas constitucionais relevantes que devem informar qualquer espécie de incursão sobre o tema. Primeiro que, embora não exista no ordenamento jurídico uma proibição absoluta para o tratamento de dados por entidades públicas, a dogmática constitucional contemporânea impõe que **a privacidade dos usuários só possa ser afastada a partir de uma justificação minudente e exaustiva das finalidades atribuídas ao tratamento de dados**.

Segundo, estabeleceu-se que a incidência do princípio da transparência impõe que a Administração Pública garanta ao titular dos dados um **nível de controle suficiente** para a verificação prospectiva da licitude do tratamento de dados. Isso se desdobraria, de acordo com a decisão, em um **dever de publicidade** que seja capaz de fornecer ao cidadão condições mínimas de proceder a um controle da forma como o Estado lida com dados pessoais.

Por fim, que a intervenção estatal na esfera privada deve (i) envolver **apenas o universo de dados estritamente necessário para o alcance das finalidades eleitas**; e (ii) ser acompanhada do **incremento dos protocolos e mecanismos de segurança do sistema de informação, de acordo com o grau de risco gerado pela relativização do direito fundamental à**

autodeterminação informativa.

Como se vê, tais diretrizes partem do pressuposto de que o **princípio da proporcionalidade** desempenha relevante papel de aferição da constitucionalidade das interferências no regime constitucional de proteção de dados, inspirando-se nas premissas assentadas no julgamento da Lei do Censo, em 1983, pelo Tribunal Constitucional alemão.

A esse respeito, conforme destacado no voto do **EMINENTE MINISTRO LUIZ FUX**, a relativização do direito fundamental somente será legítima se "*(i) atender a propósitos legítimos, específicos, explícitos e informados; (ii) limitar a coleta ao mínimo necessário para a realização das finalidades normativas; (iii) estabelecer medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais de acessos não autorizados; (iv) prevenir a ocorrência de danos, consoante os parâmetros desenhados no direito comparado e no art. 6º da Lei Geral de Proteção de Dados*".

A partir desse julgado paradigmático, o Plenário também superou a falsa ideia de que existem dados que *a priori* dispensam proteção constitucional. Em seu voto, o **EMINENTE MINISTRO RICARDO LEWANDOWSKI** explicou que informações aparentemente triviais, como o número de inscrição no CPF ou de uma linha celular, "*servem de chave de identificação e de acesso a um universo de plataformas eletrônicas, como bancos, supermercados, serviços públicos e redes sociais, todas elas detentoras das mais variadas informações sobre o titular*".

Nesse passo, de acordo com a orientação fixada pelo Tribunal, o regime constitucional de proteção de dados dispensaria considerações sobre a natureza ostensiva ou reservada dos dados pessoais. A rigor, os gatilhos que acionam o direito à autodeterminação informática relacionam-se mais propriamente com o *grau de sensibilidade das informações* e com o *risco de malversação dos dados pessoais*, tornando estéril qualquer tentativa de abrandar o nível de proteção dispensado pela ordem jurídica sob o pretexto da simplicidade ou trivialidade das informações envolvidas.

No âmbito do direito positivo, entre nós, há mais de duas décadas já

se ensaia a evolução do conceito de privacidade a partir da edição de legislações setoriais que garantem a proteção de dados pessoais, tais como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo, a Lei de Acesso à Informação, o Marco Civil da Internet – que assegura aos usuários da internet, entre outros direitos, a inviolabilidade e o sigilo do fluxo de comunicações e dos dados armazenados (art. 7º, II e III) – e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Em razão da importância da LGPD para o desfecho da controvérsia, faço breves considerações sobre o alcance e a fisionomia desse diploma normativo, destacando a posição de centralidade por ele ocupada no sistema de proteção de dados brasileiro.

A Lei 13.709/2018 dispõe sobre os princípios e procedimentos para o tratamento de dados pessoais e estabelece critérios para responsabilização dos agentes por eventuais danos ocorridos em virtude dessas atividades. Conforme lecionam Valter Shuenquener e Daniel Calil, a Lei 13.709/2018 "*teve como um de seus principais propósitos incentivar a criação de um costume institucional de proteção de dados e, especialmente por meio da Autoridade Nacional de Proteção de Dados, a preocupação de garantir a efetividade no cumprimento das normas acerca da temática* (ARAÚJO, Valter Shuenquener e CALIL, Daniel Couto dos Santos. **Inovações Disruptivas e a Proteção de Dados Pessoais: novos desafios para o Direito**, no prelo).

Com vistas a instituir uma nova cultura de gestão de dados, a LGPD parte da premissa básica de que a disciplina da proteção de dados pessoais tem como fundamento o respeito à **privacidade** e à **autodeterminação informativa** (art. 2º, incisos I e II).

Assim, dispõe que as atividades de tratamento de dados pessoais deverão observar os seguintes princípios: (i) eleição de **propósitos legítimos, específicos, explícitos** e informados ao titular; (ii) compatibilidade, ou **adequação**, do tratamento com as finalidades informadas ao titular; (iii) limitação do tratamento ao **mínimo necessário** para a realização das atividades; (iv) garantia, aos titulares, de **informações claras, precisas e facilmente acessíveis** sobre a realização

do tratamento; e (v) utilização de **medidas técnicas de segurança** aptas a proteger os dados pessoais de acessos não autorizados ou de situações ilícitas de alteração, comunicação ou difusão.

Quanto aos órgãos governamentais, a lei prevê um rol taxativo de hipóteses em que se considera legítimo o tratamento de dados por pessoas jurídicas de direito público: (i) *execução de políticas públicas* (arts. 7º e 11); e (ii) *cumprimento de atribuições institucionais*, como a execução de competências ou atribuições legais do serviço público (art. 23). A lei também exige que os agentes públicos informem *as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos* (art. 23, inciso I).

Dessa forma, percebe-se que **a LGPD parece ter limitado o tratamento de dados pelo Poder Público às atividades principais e acessórias de provisão de serviços públicos**. Uma interpretação dessa lei alinhada ao princípio constitucional da legalidade impõe, ainda, que essas finalidades conexas à prestação de serviços públicos estejam, ao máximo possível, amparadas em previsões legais específicas.

Essa trajetória de fortalecimento da tutela da privacidade culminou, recentemente, com a promulgação da Emenda Constitucional 115, de 10 de fevereiro de 2022, em que o poder constituinte derivado alçou a proteção de dados pessoais a uma autêntica condição de direito fundamental autônomo, insculpido no art. 5º, inciso LXXIX, da Constituição Federal.

Mas não só. As alterações promovidas pelo Congresso Nacional não apenas trasladaram essa garantia para o rol dos direitos fundamentais, como também atribuíram à União (i) competência material para organizar e fiscalizar a proteção e o tratamento de dados pessoais (art. 21, inciso XXVI); e (ii) competência privativa para legislar sobre proteção e tratamento de dados pessoais (art. 22, inciso XXX).

Examinando o assunto pela perspectiva da evolução do conceito de

privacidade na jurisprudência do Supremo Tribunal Federal e pelo progressivo reconhecimento, em diversas legislações setoriais, do dever estatal de tutela de informações relacionadas ao cidadão, compreende-se que a Emenda Constitucional 115/2022 teve o mérito de consolidar, de uma vez por todas, o *status* constitucional inerente ao direito de proteção de dados pessoais, dirimindo quaisquer dúvidas que pudessem pairar sobre o tema.

Todo esse panorama legislativo, doutrinário e jurisprudencial fornece uma visão holística a respeito do compromisso assumido pela ordem constitucional brasileira com a proteção de dados pessoais, fornecendo parâmetros seguros para a apreciação das controvérsias que assomam ao Plenário. Assim, é sob essa ótica de afirmação da autonomia do direito fundamental à proteção de dados pessoais que serão examinadas as alegações de inconstitucionalidade deduzidas nas ações em julgamento.

2.3 - Tratamento de dados pessoais pelo Poder Público: princípios constitucionais aplicáveis e rejeição ao isolamento do interesse público.

A discussão jurídica travada nas presentes ações de controle concentrado assume contornos próprios em relação ao debate promovido pela Corte na análise da **ADI 6.389**, de relatoria da **EMINENTE MINISTRA ROSA WEBER**. Isso se deve principalmente às complexidades que permeiam o tratamento de dados no âmbito interno da Administração Pública.

É inegável que as relações mantidas entre o Estado e os cidadãos comportam particularidades que desaconselham um simples translado do regime jurídico de proteção de dados aplicável às relações privadas. Isso se torna ainda mais evidente quando se percebe que, devido ao dinamismo das sociedades contemporâneas, a coleta, o processamento e o compartilhamento de informações biográficas constituem ferramentas indispensáveis para a verificação da eficácia e da adequação das políticas públicas que, em dado momento, compõem a agenda governamental.

Reconhecendo a essencialidade dos dados pessoais para prestação de serviços públicos, em um contexto em que a sociedade exige soluções efetivas e céleres, a professora **Miriam Wimmer** afirma que "*o tratamento de dados pessoais pelo Estado é imprescindível para o desempenho do seu mandado constitucional*". (WIMMER, Miriam. "Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público". In: DONEDA, Danilo; SARLET, Ingo Wolgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). **Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional.** Rio de Janeiro, Editora Forense, 2021, pp. 271-288).

Nesse sentido, ao lembrar que as funções do Estado recebem o influxo dos postulados inerentes ao regime jurídico de Direito Público, a autora pondera que as normas protetivas concebidas para o tratamento de dados em atividades privadas não devem ser automática e irrefletidamente aplicadas no âmbito dos órgãos estatais.

Como ressalta **Miriam Wimmer**, seria inimaginável, por exemplo, que entendêssemos que "*qualquer cidadão teria o direito de requerer ao Poder Público a portabilidade de seus dados constantes de uma determinada base de dados governamentais, ou que alguém pudesse se dirigir a um cartório para solicitar a eliminação dos seus dados pessoais ou ainda que se pretendesse negar consentimento para que a Receita Federal processasse determinada declaração de imposto de renda*" (ibidem).

Essas questões são ainda mais sensíveis no campo da segurança pública ou no das atividades de inteligência, como se discute na ADPF 695. Não faria sentido, por exemplo, condicionar a utilização de informações pessoais por órgãos de investigação ao prévio consentimento de agentes envolvidos na prática de infrações penais. Nesses casos, torna-se de fato discutível em que medida a utilidade pública envolvida no tratamento desses dados poderia impor a flexibilização das limitações previstas na legislação protetiva.

Em um contexto de rápido desenvolvimento de novas tecnologias de informação, entidades internacionais como a Organização para a Cooperação e Desenvolvimento (OCDE) têm reconhecido que a

modernização da Administração Pública, mediante a instituição de um modelo de *Data Driven Public Sector*, constitui importante passo na direção da concretização de direitos sociais (OCDE. **The Path to Becoming a Data-Driven Public Sector**. OECD Publishing: Paris, 2019).

É assente na literatura estrangeira o reconhecimento de que países comprometidos com uma agenda de um governo digital podem aprimorar os resultados de gestão utilizando novas tecnologias de forma responsiva, protetiva e transparente. Nesse aspecto, o tratamento de dados torna-se importantíssima ferramenta para o desenho, implementação e monitoramento de políticas e de serviços públicos essenciais.

Nos últimos anos, o Governo brasileiro tem buscado seguir essa agenda de digitalização da Administração Pública. Conforme será discutido adiante no presente voto, esse movimento tem sido buscado na edição de atos normativos, como o que institui o chamado Cadastro Base do Cidadão, e em programas como a Estratégia Brasileira para a Transformação Digital (e-Digital).

Dentro desse contexto, não há dúvidas de que relevantes postulados constitucionais estão em jogo quando se discutem os limites do tratamento de dados pelo Poder Público, a exemplo do princípio da eficiência da Administração Pública (art. 37, CF). Conforme destacado pela União, em sua manifestação nos autos, o compartilhamento efetivo de dados entre os órgãos e entidades da Administração Federal é, sem dúvida, pressuposto de uma gestão pública eficiente.

Todavia, diferentemente do que assevera o ente público, a **discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais**.

Como bem destacado por **Gillian 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) (BLACK, Gillian e STEVENS, Leslie. "Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest"**.** In: **Scripted**. Vol. 10, n. 1, 2013, p. 95).

Nesse sentido, assentam os autores 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.

A consciência de que os governos devem tratar o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais, é corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais.

Como destaca Daniel Solove: "*a privacidade não é algo que indivíduos automatizados possuem no estado de natureza e que sacrificam para se unir ao pacto social. Estabelecemos proteções à privacidade por causa de seus profundos efeitos sobre a estrutura de poder e de liberdade na sociedade como um todo*" (SOLOVE, Daniel. J. **Understanding Privacy**. Cambrigde: Harvard University Press, 2008, p. 93). Desse modo, assenta o autor, "*a proteção da privacidade nos protege contra prejuízos a atividades que são importantes tanto para os indivíduos quanto para a sociedade*" (Idem).

É justamente por isso que instituições como a própria OCDE têm defendido que a confiança da sociedade e a garantia de parâmetros éticos no tratamento de dados pela Administração Pública são elementares para uma boa governança dos governos digitais.

Como ressaltado pela OCDE, diversos países passaram recentemente a adotar critérios formais, definidos em legislação própria, para proteger os cidadãos no processo de coleta, armazenamento, compartilhamento e processamento de dados pelos órgãos do Estado. Em patamares de proteção mais elevados, a OCDE observa que as limitações normativas devem visar a garantir que o cidadão tenha o controle sobre: (i) quais dados as organizações governamentais têm sobre eles, (ii) quais organizações públicas têm o direito de acesso a seus dados, (iii) quais

organismos públicos fizeram uso de seus dados e para que fins, (iv) que organizações públicas fizeram um inquérito sobre seus dados e (v) o direito de concordar ou recusar permissão para que os dados que fornecem a uma instituição pública sejam compartilhados e reutilizados por outras (tradução livre) (OCDE. **The Path to Becoming a Data-Driven Public Sector**. OECD Publishing: Paris, 2019, p. 113).

Os parâmetros apontados pela OCDE parecem estar sendo constantemente perseguidos pelas nações democráticas estrangeiras. De fato, colhe-se da experiência internacional diversos modelos institucionais voltados à garantia desse patamar ético.

Uma das opções consiste na criação de entidade independente vocacionada a apoiar as entidades governamentais no gerenciamento dos dados que elas possuem sobre os cidadãos, facilitando o acesso e o compartilhamento de informações a partir de *standards* e metodologias definidos. Essa experiência tem sido concretizada em países como Irlanda, Portugal, Canadá e Nova Zelândia. Na Nova Zelândia, a propósito, o Governo instituiu um Grupo de Aconselhamento Ético para o tratamento de dados pessoais.

Outro caminho que tem sido explorado pelas nações democráticas é o estabelecimento de guias vinculantes em relação ao próprio Estado, limitando o processamento dos dados dos cidadãos. No Reino Unido, por exemplo, observa-se que as disposições da Lei Nacional de Proteção de Dados (*Data Protection Act*) são concretizadas, em múltiplos níveis, com guias e documentos orientativos, como o *Digital Economy Act*, que determina que cada Ministro expeça um código de conduta para compartilhamento de informações no âmbito de suas atribuições; e o *Data Ethics Framework*, que traz orientações bastante pragmáticas para serem utilizadas no dia a dia dos servidores públicos.

Trazendo essas considerações para a esfera local, conclui-se que compete ao Poder Público a delicada missão de delimitar adequado âmbito de proteção do direito à autodeterminação informativa, harmonizando os objetivos do Estado com os interesses legítimos dos titulares dos dados pessoais. Sobre esse ponto, destaca-se mais uma vez o

escólio de **Miriam Wimmer**:

> "A aplicação da legislação de proteção de dados no tratamento de dados pelo Poder Público – tanto no caso de atos individuais e concretos como também na edição de atos normativos – traz, portanto, o desafio de conciliação entre os princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determine a precedência *prima facie* de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual. A eficiência demandada da Administração Pública e o interesse público tutelado pelo Estado devem, portanto, ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais". (WIMMER, Miriam. "Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público". In: DONEDA, Danilo; SARLET, Ingo Wolgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). **Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional.** Rio de Janeiro, Editora Forense, 2021, pp. 271-288).

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 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 de compartilhamento de dados entre instituições públicas.

Nesse sentido, rememoro decisão proferida pela **EMINENTE MINISTRA CÁRMEN LÚCIA** na **Suspensão de Liminar 1.103 MC**, na qual determinou que o IBGE se abstivesse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças domiciliadas no município de Bauru/SP, que,

de acordo com o Censo realizado em 2010, não teriam sido regularmente registradas nos Cartórios de Registro Civil de Pessoas Naturais. Nessa decisão, a então Presidente do Supremo Tribunal Federal afirmou a necessidade de conciliação dos valores constitucionais em jogo ao pontuar:

> "**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. 1.611/1967 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 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". (SL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017).

No mesmo sentido, destaco decisão proferida pelo **EMINENTE MINISTRO LUÍS ROBERTO BARROSO** nos autos do **Mandado de Segurança 36.150 MC**, na qual cassou 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, com o fim de realizar auditoria do Programa Bolsa Família.

Nessa importante decisão, o eminente relator dialogou profundamente com a noção de finalidade aqui discutida, apontando risco de subversão da autorização concedida pelos titulares dos dados pessoais no ato de coleta. Destaco trecho da referida decisão:

> "7. É certo que o art. 71, IV, da Constituição confiou ao TCU a competência para a realização de inspeções e auditorias de natureza contábil, financeira, orçamentária, operacional e patrimonial nos órgãos e entidades da Administração. A atribuição dessa competência, por óbvio, supõe o reconhecimento dos meios necessários ao cumprimento desse encargo. Isso inclui a prerrogativa de requerer aos responsáveis pelos órgãos e entidades as informações necessárias à instrução de processos de auditoria e inspeção. No caso, no entanto, as informações que se quer acessar foram prestadas para uma finalidade declarada no ato da coleta dos dados e sob a garantia de sigilo do INEP quanto às informações pessoais. 8. Nesse aspecto, **a transmissão a outro órgão do Estado dessas informações e para uma finalidade diversa daquela inicialmente declarada subverte a autorização daqueles que forneceram seus dados pessoais, em aparente violação do dever de sigilo e da garantia de inviolabilidade da intimidade**. De igual modo, é plausível a alegação de que a franquia desses dados quebra a confiança no órgão responsável pela pesquisa por violação do sigilo estatístico. Há, pois, risco à própria continuidade das atividades desempenhadas pelo INEP, com efetivo prejuízo ao monitoramento das políticas públicas de educação". (**MS 36.150 MC**, Rel. Min. Roberto Barroso, julgado em 10.12.2018, DJe 13.12.2018).

Assim, é clara a necessidade de temperar os valores constitucionais da eficiência da Administração Pública com o regime constitucional de tutela dos direitos individuais, particularmente as garantias de autodeterminação informativa e de proteção dos dados pessoais (art. 5º, *caput* e incisos X, XII e LXXIX, da Constituição Federal).

2.4 - Objeto da ADPF 695. Compartilhamento de dados pessoais para realização de atividades de inteligência

Considero apropriado iniciar pelo exame do ato de compartilhamento impugnado na Arguição de Descumprimento de Preceito Fundamental 695. Assim o faço porque as distorções e irregularidades identificadas da ação administrativa impugnada na ADPF auxiliam na constatação do quadro geral de insegurança que deriva do regulamento editado pelo Poder Executivo, o Decreto 10.046/2019.

Na ADPF 695, o Partido Socialista Brasileiro (PSB) requer seja sanada grave lesão a preceitos fundamentais, consistente no "*compartilhamento de dados pessoais (...) pelo Serviço Federal de Processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN), com suposto lastro normativo no Decreto 10.046, de 9 de outubro de 2019*". Sustenta, em síntese, que a "*transferência massiva e indiscriminada dos dados pessoais de todos os portadores de CNH no país para a Agência Brasileira de Inteligência*" viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa.

Atento ao risco de violação massiva à proteção de dados pessoais de 76 milhões de brasileiros, requeri, no dia 22.6.2020, a apresentação da ADPF 695 em mesa para apreciação do pedido de concessão da medida cautelar. Em homenagem ao princípio da colegialidade, pretendi submeter a controvérsia ao crivo do Tribunal Pleno, visando promover um debate plural acerca da compatibilidade do ato do Poder Público com o regime constitucional de proteção de dados pessoais.

Ocorre que, no dia 23.6.2020**, às vésperas da sessão de julgamento,** a AGU peticionou nos autos informando a revogação do Termo de Autorização que concedera o acesso da ABIN à base de dados da Carteira Nacional de Habilitação. Requereu, então, fosse declarada a perda de objeto da ADPF.

A partir dessa provocação, os autos retornaram ao meu gabinete, ocasião em que ponderei que, sem embargo da revogação do termo de

autorização, o ato do Poder Público impugnado nesta ADPF abrangia todo um quadro de insegurança jurídica gerado por leituras distorcidas do Decreto 10.046/2019. Por esse motivo, reconheci que persistia interesse processual quanto ao pedido de interpretação conforme do regulamento administrativo.

Assim, proferi decisão no dia 24 de junho de 2020, reconhecendo que, não fosse o abandono do intento de transferência massiva e indiscriminada de dados pessoais para a Agência Brasileira de Inteligência, a União enfrentaria grandes dificuldades para sustentar a constitucionalidade da medida perante o Supremo Tribunal Federal. Nessa senda, apontei que a **redação genérica** do ato impugnado erigia obstáculos intransponíveis ao exercício do controle judicial, sobretudo por não indicar as finalidades pretendidas pelo órgão solicitante nem a real necessidade de utilização de informações de 76 milhões de brasileiros em atividades de inteligência. Eis o que assentei na ocasião:

> No caso em tela, há uma enorme dificuldade em proceder ao teste de proporcionalidade em todas as suas etapas. Como dito, o único ato material submetido a um mínimo de publicidade consiste no Termo de Autorização 7/2020 e no extrato do mencionado Termo de Autorização, publicados no Diário Oficial da União – DOU 46, Seção 3, de 9 de março de 2020.
>
> Embora a União afirme que este Termo de Autorização "foi emitido de modo completamente transparente, em veículo da imprensa oficial, segundo o procedimento aplicado às solicitações de mesma natureza", não é possível colher do extrato publicado no Diário Oficial da União qualquer informação relevante sobre a natureza dos dados compartilhados tampouco acerca dos parâmetros objeto do compartilhamento.
>
> Ressalte-se que, por disposição expressa do art. 5º do Decreto 10.046/2019, "fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de dados entre os órgãos".

> Assim, dificilmente os órgãos envolvidos no compartilhamento tornariam público no futuro os termos em que o compartilhamento ocorreria.
>
> [...]
>
> Assim, do ponto de vista da adequação, seria bastante difícil examinar o ato em questão, já que a única face pública da medida impugnada adota redação genérica para indicar os objetivos do compartilhamento de dados e nem sequer explicita a finalidade pretendida com as atividades de inteligência.
>
> Já sob o prisma da necessidade, diante da ausência de explanação da finalidade do compartilhamento, torna-se impossível aferir se o compartilhamento na dimensão apresentada se revela o meio menos intrusivo possível para alcançar o objetivo apresentado. Aqui talvez seja o elemento em que recai o maior ônus da Administração Pública: explicar por que afinal seria necessário o processamento de dados da CNH de 76 milhões de brasileiros para atividades de inteligência.
>
> Por fim, ainda que fosse possível avançar no juízo da proporcionalidade em sentido estrito, dificilmente seria possível compatibilizar uma violação massiva à proteção de dados pessoais, traduzida no compartilhamento irrestrito de dados da CNH de mais de 76 milhões de brasileiros, com alguma finalidade legítima de tratamento de dados para atividades de vigilância.
>
> Por todos esses motivos, entendo que, no caso concreto, há significativa e densa verossimilhança nas alegações do autor, no sentido de que o ato do Poder Público trazido a exame por esta Suprema Corte (i) tem o potencial de violar os preceitos fundamentais da proteção da privacidade, da proteção de dados e da autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII, da CF/88); (ii) não possui base normativa que eventualmente lhe ampare – o que poderia em tese lhe emprestar legitimidade; e (iii) tampouco mostra-se proporcional ante as suas finalidades.

Essas considerações são necessárias para demonstrar que, a despeito

do abandono dos propósitos inicialmente almejados pela ABIN, ainda persistem graves riscos para a tutela da privacidade e da autodeterminação informativa.

O tema de fundo da ADPF conduz à inescapável percepção da insegurança gerada pela abertura semântica do Decreto 10.046/2019, que, não raras vezes, tem desaguado em leituras desviantes e extremamente alargadas do seu programa normativo, com manifestos prejuízos para o regime constitucional de proteção de dados pessoais.

Sem maiores digressões, apenas para mencionar o caso específico tratado na ADPF, causa perplexidade que, na defesa apresentada nos autos, a União sustente que o compartilhamento pretendido pela ABIN encontra suporte normativo no inciso I do art. 3º do Decreto 10.046/2019, cujo teor assim dispõe:

> Art. 3º – O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> I – a informação **do Estado** será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais.

Tal linha de pensamento, entretanto, me parece em frontal choque com os lineamentos mais basilares do postulado do Estado Democrático de Direito; confronta, outrossim, com os limites que decorrem do texto constitucional para o tratamento de dados pessoais (bem como da legislação ordinária veiculada pelo Congresso Nacional, no exercício de sua competência para atuar nesse âmbito facultado).

São duas as razões que me conduzem a essa conclusão. A **primeira** diz respeito à necessidade de promover uma leitura do regulamento administrativo alinhada com o regime constitucional de tutela da privacidade. Trata-se de assunto que será devidamente aprofundado ao longo do presente voto, cabendo, contudo, desde já registrar que o sentido do Decreto 10.046/2019 que melhor traduz os objetivos da ordem

constitucional conduz ao abandono de qualquer interpretação que possibilite um amplo e irrestrito compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública Federal.

Assim, sem me antecipar em relação ao aprofundamento do tema, registro que, em homenagem ao direito à autodeterminação informativa, apenas as **informações gerais do Estado** são alcançadas pelo disposto no art. 3, inciso I, do Decreto 10.046/2019, e não aquelas relacionadas aos atributos da personalidade ou qualidades próprias do cidadão.

Devem ser amplamente compartilhadas, nos termos do dispositivo, somente as informações relativas ao funcionamento do aparato estatal, como gestão de pessoal e do patrimônio público, utilização de recursos orçamentários, formalização de atos e contratos administrativos, apenas para citar alguns exemplos. Lado outro, em relação às informações pessoais, devem incidir os vetores protetivos da LGPD, estruturados para a salvaguarda da privacidade dos cidadãos, que exigem o preenchimento de requisitos mais rígidos para o fluxo de informações no âmbito dos órgãos públicos federais.

A **segunda** razão para rejeitar a tese deduzida pela União diz respeito à impossibilidade de invocação dos dispositivos do Decreto 10.046/2019 e da Lei 13.709/2018 para legitimar operações de tratamento de dados no âmbito do Sistema Brasileiro de Inteligência. Afinal, basta um simples lançar de olhos sobre o art. 4º, inciso III, da Lei 13.709/2018 para concluir que o compartilhamento de dados pessoais para fins de defesa nacional "***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***".

Ao que tudo indica, considerando a sensibilidade das atividades relacionadas à preservação da soberania nacional, o legislador entendeu que o assunto deveria observar **legislação específica**, adequada às particularidades desse campo de atuação estatal. Antecipou, contudo, que esse regime especial de tratamento de dados deve ser calibrado à luz dos pilares estruturantes da LGPD, especialmente no que diz respeito à

necessidade de apresentação de justificação minudente das finalidades pretendidas pelos órgãos de inteligência.

Esse tema foi exaustivamente debatido na **ADI 6.529**, de relatoria da **EMINENTE MINISTRA CÁRMEN LÚCIA**, DJe de 22.10.2021, em que esta Corte assentou que, desde que observados os requisitos legais, é legítimo o compartilhamento de conhecimentos específicos com a Agência Brasileira de Inteligência, na forma do parágrafo único do art. 4º da Lei 9.883/1999.

Na ocasião, o Tribunal conheceu parcialmente da ação para conferir interpretação conforme ao mencionado dispositivo, estabelecendo que (a) o compartilhamento de dados no âmbito do Sistema Brasileiro de Inteligência somente pode ocorrer quando demonstrado o **interesse público da medida**; (b) toda e qualquer decisão de fornecimento de dados deverá ser **devida e formalmente motivada** para eventual controle de legalidade pelo Poder Judiciário; c) mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo legal; e d) são indispensáveis a **instauração de procedimento administrativo formal** e a **utilização de sistemas eletrônicos de segurança e registro de acesso**, para efeito de responsabilização em caso de abuso.

Desse panorama, extraem-se duas importantes conclusões. **Primeiro**, ao contrário do afirmado pela União, as disposições da LGPD e do respectivo decreto regulamentador não constituem, *per se,* suporte legal para o compartilhamento de dados pessoais no âmbito do Sistema Brasileiro de Inteligência. Em **segundo lugar**, embora seja possível o compartilhamento de conhecimentos específicos com a ABIN, isso não afasta necessidade de se examinar, sob a perspectiva constitucional, se as restrições impostas pelo ato administrativo estão devidamente motivadas e se atendem, ou não, às balizas fixadas no julgamento da **ADI 6.529, de relatoria da EMINENTE MINISTRA CÁRMEN LÚCIA**.

Feitas essas considerações, entendo que, sem embargo da revogação do Termo de Autorização 07/2020, o grave quadro de insegurança jurídica

causado pela elasticidade semântica do Decreto 10.046/2019 evidencia a necessidade de realizar o julgamento da ADPF 695 em conjunto com a ADI 6.649.

Cuida-se de rica oportunidade para o Tribunal avaliar, em perspectiva global, se o sentido atribuído pela Administração Pública ao referido decreto regulamentar se compatibiliza, ou não, com a ordem constitucional brasileira.

2.5 - Confronto do programa normativo do Decreto 10.046/2019 com a Constituição Federal

A controvérsia abordada na Ação Direta de Inconstitucionalidade 6.649/DF diz respeito, essencialmente, à validade dos dispositivos do Decreto 10.046, de 9 de outubro de 2019, que *dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados*.

O regulamento impugnado desempenha a delicada missão de sistematizar regras e princípios aplicáveis ao compartilhamento de dados entre órgãos públicos federais, em uma tentativa de fundar balizas para aplicação harmônica dos dispositivos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) e da Lei de Acesso à Informação (Lei 12.527/2011). A complexidade do assunto é evidenciada pela existência de **conflitos aparentes** entre normas que impõem transparência absoluta na condução dos negócios públicos, de um lado, e aquelas que estabelecem limites rigorosos para o fluxo de **dados pessoais** coletados ou produzidos pelo Estado, de outro.

Se é certo que **informações gerais relacionadas à atividade administrativa** devem, em regra, se submeter ao princípio da ampla publicidade**,** não é menos exato que o tratamento de **dados pessoais** segue lógica diversa, focada na salvaguarda da privacidade dos cidadãos. Essa distinção impõe **regime jurídico híbrido** para o tratamento das informações coletadas ou produzidas pela Administração Pública, a depender do maior ou menor vínculo que elas guardem com **atributos da**

personalidade ou **qualidades próprias do cidadão.**

Não há, evidentemente, como ombrear o regime jurídico restritivo que orienta o tratamento de dados pessoais, fundado em vetores protetivos, com as regras e princípios que se aplicam ao manuseio de informações relacionadas ao próprio funcionamento do aparato estatal, como despesas administrativas, atos de gestão do patrimônio público, licitações, contratos administrativos, pareceres e decisões administrativas, apenas para citar alguns exemplos.

Dadas a complexidade da matéria e as incertezas e aflições que fatalmente incidiriam sobre os agentes responsáveis pela aplicação da lei, impunha-se a construção de balizas interpretativas que fossem capazes de acomodar, em um mesmo programa normativo, o dever geral de publicidade dos negócios públicos e o regime constitucional de proteção de dados pessoais.

Nesse contexto, surge o Decreto 10.046/2019 como uma tentativa de orientar a atuação dos servidores públicos responsáveis pela governança de dados na Administração Pública Federal, sobretudo no que se refere à interoperabilidade e integração dos bancos de dados mantidos pelos diferentes órgãos e entidades que a compõem.

O regulamento impugnado pode ser decomposto em quatro eixos normativos. O primeiro deles, contido nos arts. 1º a 3º, arrola os objetivos que devem orientar o compartilhamento de dados na Administração Pública Federal, com destaque para a simplificação da oferta de serviços públicos, a avaliação e o monitoramento constante da eficiência das políticas públicas e a melhoria da qualidade e integridade dos dados custodiados pelos órgãos federais. Adicionalmente, ao dispor sobre as diretrizes que devem ser observadas nessas operações, o decreto impõe o compartilhamento da informação do Estado da forma mais ampla possível, ao mesmo tempo que assegura a observância da Lei Geral de Proteção de Dados (art. 1º, inciso I).

Outro eixo, delineado nos arts. 4º a 14, estabelece três níveis de compartilhamento de informações, quais sejam: (i) **compartilhamento amplo**, quando se tratar de dados públicos que não estejam sujeitos a

nenhuma restrição de acesso, cuja divulgação deve ser ampla e garantida a qualquer interessado (art. 4º, inciso I); (ii) **compartilhamento restrito,** para dados sigilosos que, pela sua natureza, possam ser acessados por todos os órgãos e entidades da Administração Pública Federal (art. 4º, inciso II); e (iii) **compartilhamento específico**, quando se tratar de dados protegidos por sigilo que, pelo grau de sensibilidade, somente podem ser repassados a órgãos e entidades específicos, nas hipóteses e para os fins previstos em lei (art. 4º, inciso III).

O terceiro eixo, contido nos arts. 16 a 20, institui o **Cadastro Base do Cidadão**, mecanismo de interoperabilidade voltado ao aprimoramento da gestão de políticas públicas e ao aumento da confiabilidade dos cadastros existentes. Cuida-se de repositório unificado que funcionará conforme a política de governança aprovada pelo Comitê Central de Governança de Dados e que será composto, inicialmente, pelas informações biográficas que constam da base temática do CPF.

Por fim, o quarto eixo, delineado nos arts. 21 e seguintes, prevê a estrutura e a forma de funcionamento do **Comitê Central de Governança de Dados**, a quem compete fixar orientações e diretrizes para a categorização do compartilhamento amplo, restrito e específico; e, ainda, dispor sobre a arquitetura, os requisitos de acesso e a política de segurança do Cadastro Base do Cidadão.

Pois bem. Alega o requerente que, a pretexto de regulamentar diplomas normativos diversos, o regulamento administrativo: a) invadiu competência privativa do Congresso Nacional e exorbitou o poder regulamentar conferido ao Presidente da República; b) dispôs sobre a matéria de forma contrária aos preceitos constitucionais e infraconstitucionais relacionados à proteção de dados e da privacidade; e c) instituiu um cadastro unificado que poderá ser utilizado abusivamente pelos órgãos do poder público federal, além de acarretar riscos de vazamentos e incidentes de segurança.

Embora a Ação Direta tenha como propósito a declaração de inconstitucionalidade da íntegra do Decreto 10.046, de 9 de outubro de 2019, o raciocínio articulado na petição inicial revela que o desconforto do

requerente reside principalmente na disciplina dos níveis de compartilhamento de dados pessoais, na instituição do Cadastro Base do Cidadão e no delineamento do Comitê Central de Governança de Dados. Há receio de que o texto do regulamento possa dar margem a um fluxo desordenado de dados pessoais no âmbito do Poder Executivo, em desacordo com as disposições da LGPD.

Surge, em boa hora, uma alvissareira oportunidade para que o Tribunal, no contexto do compartilhamento de dados entre órgãos e entidades integrantes da Administração Pública, reflita não apenas sobre as salvaguardas institucionais que devem acompanhar o tratamento de dados por órgãos governamentais, como também sobre os limites do poder regulamentar em matéria de privacidade e proteção de dados.

Pois bem. A despeito da complexidade ímpar da matéria, penso que, *a priori*, assiste ao Presidente da República competência para produzir os parâmetros de uniformização necessários à execução da Lei Geral de Proteção de Dados Pessoais pelos órgãos e entidades federais.

A rigor, em se tratando de leis que são objeto de ação administrativa, a expedição de regulamentos constitui providência essencial para o bom funcionamento da estrutura orgânica da Administração Pública Federal. Por meio deles, o Presidente da República não apenas fixa critérios uniformes para a aplicação da legislação pelos órgãos integrantes do aparelho estatal, como também afasta dúvidas e dificuldades que poderiam comprometer a operatividade da lei.

Não por outra razão, doutrinadores de renome preferem substituir a expressão *poder regulamentar* por *dever regulamentar*, que melhor enfatiza a responsabilidade do Chefe do Poder Executivo de instituir normas secundárias necessárias para a fiel execução da lei, impedindo o surgimento de incertezas que possam implicar paralisia administrativa. A esse respeito, a professora **Maria Sylvia Zanella Di Pietro** alerta que, "*embora o vocábulo* ***poder*** *dê a impressão de que se trata de faculdade da Administração, na realidade trata-se de* ***poder-dever****, já que reconhecido ao poder público para que o exerça em benefício da coletividade; os poderes são, pois, irrenunciáveis*". (**Manual de Direito Administrativo.** 14ª ed. São Paulo:

Atlas, 2018, p. 115)

No que diz respeito ao tratamento de dados pelo poder público, verifica-se que diversos dispositivos da Lei 13.709/18 pressupõem vigorosa atuação de órgãos administrativos para execução do que neles se dispõe. O legislador, no entanto, dada a generalidade e o caráter abstrato da lei, não foi capaz de dispor sobre todos os aspectos da política legislativa de proteção de dados pessoais, em especial no que concerne à administração das informações biográficas coletadas pelo Estado. Subsiste, então, a necessidade de expedição de normas secundárias para orientar os agentes públicos sobre como proceder diante dessa delicada tarefa.

Deparamo-nos, portanto, com exemplo típico de programa normativo cuja operatividade depende de ulterior regulamentação pelo Chefe do Poder Executivo, por meio da fixação dos parâmetros necessários para aplicação consistente e uniforme da lei. No caso da LGPD, são muitas as normas que impõem ações concretas do Estado em matéria de gestão de dados pessoais e, nessa medida, reclamam a edição de atos complementares para densificação dos princípios gerais por ela estabelecidos.

Destaco, pela pertinência com a demanda, os dispositivos que determinam a manutenção de bases temáticas em plataformas integradas, estruturadas para uso compartilhado; e os que orientam os gestores públicos a desenvolverem mecanismos eletrônicos de interoperabilidade**,** com a finalidade de aumentar a confiabilidade dos cadastros administrativos, aprimorar a gestão de políticas públicas e permitir a atuação articulada dos órgãos estatais na prestação de serviços públicos.

É o que dispõem os arts. 25 e 26 da Lei Geral de Proteção de Dados Pessoais:

> Art. 25. **Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado**, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público geral.

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de **execução de políticas públicas** e **atribuição legal** pelos órgãos e pelas entidades públicas, **respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.**

No mesmo sentido, destaco que a moderna Lei 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital, prevê como um dos seus princípios a "***atuação integrada entre os órgãos e as entidades envolvidos na prestação e no controle de serviços públicos***, *com o* ***compartilhamento de dados pessoais*** *em ambiente seguro quando for indispensável para a prestação do serviço,* ***nos termos da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)*** *[...]".*

Mais adiante, a Lei do Governo Digital assim estabelece:

> Art. 39. **Será instituído mecanismo de interoperabilidade com a finalidade de**:
>
> I - aprimorar a gestão de políticas públicas;
>
> II - aumentar a confiabilidade dos cadastros de cidadãos existentes na administração pública, por meio de mecanismos de manutenção da integridade e da segurança da informação no tratamento das bases de dados, tornando-as devidamente qualificadas e consistentes;
>
> III - viabilizar a criação de meios unificados de identificação do cidadão para a prestação de serviços públicos;
>
> IV - facilitar a interoperabilidade de dados entre os órgãos de governo;
>
> V - realizar o tratamento de informações das bases de dados a partir do número de inscrição do cidadão no CPF, conforme previsto no art. 11 da Lei nº 13.444, de 11 de maio de 2017.
>
> Parágrafo único. Aplicam-se aos dados pessoais tratados por meio de mecanismos de interoperabilidade as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção

de Dados Pessoais).

Nossa legislação federal, portanto, contempla um plexo de disposições normativas que impõem à Administração Pública a difícil tarefa de **implementar bancos de dados de natureza interoperável, desenvolvidos para permitir o compartilhamento eletrônico de informações entre órgãos governamentais**, **sem prejuízo da irrestrita observância dos princípios gerais e mecanismos de proteção elencados na Lei Geral de Proteção de Dados Pessoais.**

Há um outro aspecto fundamental que não pode ser olvidado pela Corte. Mesmo que ausentes os referidos comandos legais, é certo que a Constituição Federal impõe ao Estado o dever de desenvolver a atividade administrativa do modo mais eficiente, mais econômico e mais adequado ao interesse público. Naturalmente, o cumprimento da determinação constitucional pressupõe emprego das mais modernas tecnologias e soluções computacionais, sobretudo em um contexto de amplo desenvolvimento de ferramentas digitais, de modernas aplicações de informática e de computação em nuvem (*cloud computing*).

É impensável que, na sociedade moderna, as repartições públicas operem com instrumentos defasados, renunciando à tecnologia, às ferramentas digitais, e desprezando as melhores práticas gerenciais. Ou seja, não é dado ao Estado virar as costas para o progresso tecnológico, tampouco permanecer amarrado ao passado. Cuida-se de mais cristalina aplicação do princípio da eficiência administrativa, ou daquilo que os italianos chamam de *princípio da boa administração*. (CLARICH, Marcello. **Manuale di Diritto Amministrativo**. 5ª ed. Bolonha: il Mulino, 2022, pp. 152-153)

Isso não quer dizer que o dever de eficiência sirva de manobra para o descumprimento do princípio da legalidade nem que constitua um cheque em branco para o administrador público. Revela, apenas, a assunção de um compromisso de eficiência e busca dos melhores resultados pelo Estado brasileiro, o que **de modo algum** representa uma licença para o desatendimento dos preceitos éticos que informam o regime constitucional, entre eles os mecanismos de proteção de dados

pessoais.

São diversos os exemplos de emprego de ferramentas tecnológicas no interesse do cidadão e da eficiente prestação de serviços públicos. Apenas para citar um caso, destaco portaria recente do Ministro do Trabalho e Previdência que, em benefício de idosos ou de pessoas com deficiência, dispensa segurados do INSS ou beneficiários do Benefício de Prestação Continuada (BPC) de comparecerem presencialmente às agências do INSS ou agências bancárias para realização da assim chamada *prova de vida* (Portaria MTP 220, de 2 de fevereiro de 2022).

A partir de agora, a Administração Pública se valerá de mecanismos menos intrusivos, como o compartilhamento de dados, para evitar pagamentos indevidos a pessoas falecidas e combater fraudes no âmbito da seguridade social. Por meio de integração de bases de dados, informações que já se encontram em posse de órgãos públicos federais serão utilizadas para dispensar a *prova de vida*. Basta que o cidadão tenha sacado dinheiro em agências bancárias, solicitado renovação de carteira de identidade ou habilitação, passaporte ou registro de votação, para que seja considerado vivo. Deparamo-nos, aqui, com exemplo real de legítima utilização do compartilhamento de dados em benefício do cidadão.

A propósito, registro que as informações prestadas pela Presidência da República demonstram, em geral, os propósitos que orientaram a edição do Decreto 10.046/2019 e, no particular, a preocupação do Poder Executivo com a preservação da privacidade dos titulares de dados pessoais. Destaco:

> "O Decreto n. 10.046/2019 permite a gestão e o uso de dados já gerados nos sistemas da Administração Pública Federal de forma a garantir qualidade da informação, com o uso da tecnologia para promover eficiência nos processos, bem com **garantir a segurança da informação através de critérios previstos pelo próprio Decreto e com base na Lei Geral de Proteção de Dados – LGPD (vide artigo 5º do Decreto n.º 10.046/2019).**
>
> [...] Trata-se de um mecanismo essencial para a

autenticação digital, que reduz a ocorrência de falsificação ideológica e duplicação de identificação, o que evidentemente evita fraudes e estelionatos. Além disso, traz maior confiabilidade em operações, inclusive transações financeiras, simplifica e automatiza procedimentos de prova de vida, identificação, reduzindo custos e riscos no fornecimento de serviços públicos. Outros benefícios dos dados biométricos são a desduplicação de cadastros do governo, trazendo qualidade e unicidade dos dados. Todas essas medidas devem ser pautadas em tecnologia de segurança da informação, a fim de garantir a eficiência na execução de serviços públicos.

[...]

Tendo em vista a pluralidade de bases de dados já custodiadas pelo Estado, é crucial a interoperabilidade entre elas para fins, dentre outros, de **cruzamento dos dados nela existentes**. Frequentemente, tais dados se referem à mesma pessoa física ou jurídica, mas revelam informações contraditórias. Com isso, é inviabilizado o acesso a serviços públicos a cidadãos que fariam jus a benefícios. **Analogamente, essa inconsistência poderia implicar a concessão de acesso a pessoas que, por sua vez, não estariam legalmente habilitadas.** A inconsistência entre bases de dados tem tais efeitos práticos, em detrimento da celeridade e da correta prestação de bens e serviços públicos. Essas inconsistências nas bases de dados foram amplamente analisadas por recentes acórdãos do Tribunal de Contas da União. Destacam-se, nesse sentido, o Acórdão n.º 1.706/2020, que analisou o compartilhamento de dados para validação do pagamento do auxílio emergencial, e o Acórdão n.º 1.123/2020, que analisou divergências entre diversas bases de dados do governo federal.

Essas incongruências nas concessões de serviços públicos geram distorções que afrontam o princípio da isonomia de tratamento, que deve nortear as ações públicas. **Em um cenário ainda mais negativo, essas inconsistências podem causar prejuízo ao erário: a concessão de benefício, por exemplo, a quem não está apto a recebê-lo gera, muitas das vezes, a não**

> **concessão desse mesmo benefício a quem o detém de direito – em um contexto de limitações orçamentárias e financeiras de recursos públicos federais".**

Não há como negar que o texto da norma impugnada é fiel aos propósitos elencados nas informações prestadas pela Presidência da República. A moldura semântica do decreto presidencial revela compromisso do Estado brasileiro com adoção de ferramentas tecnológicas capazes de aprimorar a prestação de serviços públicos e aumentar a eficiência da atividade administrativa, **ao mesmo tempo que prestigia as normas e princípios previstos na Lei Geral de Proteção de Dados Pessoais.**

Longe de indicar um preciosismo redacional, as inúmeras remissões que são feitas às regras e princípios instituídos pela LGPD são cruciais para o desfecho da presente controvérsia. São elas que me conduzem à certeza de que as disposições do decreto presidencial não contêm nenhuma permissão expressa para compartilhamento de dados pessoais de maneira ampla e irrefletida, fora do eixo de proteção instituído pela Lei 13.709/2018.

E isso por um simples motivo. Em razão do constante diálogo que o decreto presidencial promove com as normas protetivas de dados pessoais, seu programa normativo, **quando interpretado com razoabilidade**, sinaliza para um **duplo padrão de tratamento** das informações custodiadas em poder da Administração Pública.

De um lado, para as **informações gerais do Estado**, vigora regime mais flexível e maleável, focado no acesso à informação e no controle social da atuação estatal. E, de outro, no que diz respeito aos **dados pessoais**, prevalece regime mais rigoroso, voltado fundamentalmente para a proteção do indivíduo em face do risco de malversação de seus atributos biográficos.

Quanto às primeiras, o decreto contempla previsões genéricas, fundadas na Lei 12.527/2011 (Lei de Acesso à Informação), no sentido de impor (a) ampla divulgação, preferencialmente em canais de dados abertos e de transparência ativa, de **informações públicas**, a exemplo de

despesas administrativas, estrutura de pessoal, estatísticas oficiais e documentos públicos (art. 4º, inciso I); e (b) compartilhamento parcimonioso de **informações sigilosas do Estado**, restrito a órgãos e entidades que compõem a Administração Pública Federal, nos termos da legislação (art. 4º, incisos II e III).

Por outro lado, sempre que menciona ou tangencia especificamente a temática do tratamento de **dados pessoais**, o decreto presidencial tem o cuidado de determinar a **incondicional observância dos princípios gerais e direitos de proteção elencados na LGPD e dos direitos constitucionais à privacidade e proteção de dados**. A propósito, assim dispõem os arts. 3º, incisos I e V, 5º, *caput*, e 21, inciso I, e 26, §1º:

> **Art. 3º** O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> **I -** a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações **e o disposto na Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais**;
>
> [...]
>
> **V -** nas hipóteses em que se configure tratamento de **dados pessoais**, serão observados o **direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação**; e
>
> VI - a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018;
>
> [...]
>
> **Art. 5º** Fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para efetivação do compartilhamento de dados entre os órgãos e as entidades de que trata o art. 1º, observadas as diretrizes do art. 3º e o **disposto na Lei nº 13.709, de 2018.**
>
> [...]

> **Art. 21**. Fica instituído o Comitê Central de Governança de Dados, a quem compete deliberar sobre:
>
> **I -** as orientações e as diretrizes para a categorização de compartilhamento amplo, restrito e específico, e a forma e o meio de publicação dessa categorização, **observada a legislação pertinente, referente à proteção de dados pessoais.**
>
> [...]
>
> **Art. 26.** As controvérsias no compartilhamento de dados entre órgãos e entidades públicas federais solicitantes de dados e o gestor de dados serão decididas pelo Comitê Central de Governança de Dados.
>
> **§1º** As resoluções do Comitê Central de Governança de Dados a respeito de controvérsias **observarão as normas que protegem os dados objetos de controvérsia**.

Qualquer interpretação desviante dessa lógica, no sentido de possibilitar ampla, irrestrita e irresponsável difusão dos dados pessoais custodiados pelo Estado, conflita não apenas com diversas previsões expressas do próprio decreto presidencial, mas principalmente com preceitos sensíveis que compõem a espinha dorsal da Constituição da República e da Lei Geral de Proteção de Dados Pessoais, como os direitos à privacidade e à autodeterminação informativa.

Esse mesmo espírito deve guiar a construção e o funcionamento do Cadastro Base do Cidadão. Tenho para mim que, desde que interpretados de maneira sistemática e em conformidade com as regras da LGPD, os dispositivos do Decreto 10.046/2019 **não** abrem espaço para a instituição de uma base integradora descomunal, nos moldes temidos pelos requerentes.

Muito pelo contrário. Embora seja permitida e até mesmo necessária a instituição de instrumentos de interoperabilidade aptos a simplificar o fluxo de dados entre órgãos públicos, as inúmeras alusões feitas pelo decreto ao regime protetivo instituído pela LGPD impõem a necessidade de estabelecimento de **ferramentas rigorosas de controle de acesso** ao Cadastro Base do Cidadão.

Qualquer tentativa de abertura ampla dos elementos nele contidos,

mesmo que restrita ao conjunto de órgãos públicos federais, conflitaria frontalmente com as normas que orientam o tratamento de dados pessoais. Nesse sentido, os arts. 6º, 7º e 23 da Lei 13.709/2018 estabelecem procedimento específico para o compartilhamento de dados pessoais pelo Poder Público, prevendo que, **para cada entidade interessada no tratamento de informações protegidas**, sejam apresentados (i) propósitos legítimos; (ii) compatibilidade do tratamento com as finalidades informadas; e (iii) limitação do compartilhamento ao mínimo necessário para atendimento do interesse público.

2.6 – Distorções na composição do Comitê Central de Governança de Dados.

Considerando a relevância das atribuições exercidas pelo Comitê Central de Governança de Dados, é preciso refletir com cautela sobre as normas que estabelecem a composição do colegiado e a forma de indicação de seus membros.

Entre os argumentos articulados na petição da ADI 6.649, encontra-se a alegação de que o Decreto 10.046/2019 limita a participação no Comitê Central de Governança a "*funcionários da administração direta federal (art. 22), sem qualquer previsão de composição multissetorial*". Pondera, ainda, que se trata "*de um desenho institucional inadequado para promover a segurança, a necessidade, a adequação e a boa-fé no compartilhamento e utilização das informações pessoais*".

A esse respeito, entendo que os argumentos lançados pelo requerente são capazes de demonstrar que o Comitê Central de Governança de Dados, na forma como estruturado pelo Decreto 10.046/2019, não apenas oferece **proteção deficiente** para valores centrais da ordem constitucional, como também constitui **fator de desestabilização** das garantias previstas na Lei 13.709/2018.

Há, atualmente, um certo consenso acerca da necessidade de criação de autoridades administrativas **independentes**, destacadas especificamente para fiscalização e controle de atividades potencialmente

lesivas ao direito de privacidade. São órgãos que desempenham papel fundamental para a concretização e o êxito das políticas de proteção enunciadas no direito positivo, constituindo fio condutor do regime constitucional de proteção de dados pessoais.

A experiência internacional nos mostra que, desde os primeiros ensaios de proteção desse direito fundamental, os países europeus reconheceram a necessidade de criação de uma ou mais autoridades independentes para monitoramento e supervisão das operações de tratamento de dados pessoais.

Já em de 25 de outubro de 1995, a **Diretiva 95/46 do Parlamento Europeu** dispunha que as autoridades públicas responsáveis pela fiscalização das atividades de tratamento de dados "*exercerão com* ***total independência*** *as funções que lhes forem atribuídas*". Posteriormente, em 7 de dezembro de 2000, a **Carta dos Direitos Fundamentais da União Europeia** estabeleceu, ao lado da consagração do direito fundamental à proteção de dados pessoais, a necessidade de que *o cumprimento dessas regras fique sujeito à fiscalização por parte de uma autoridade* ***independente*** (art. 8º).

A seu turno, o **Regulamento Geral sobre Proteção de Dados** (GPDR, na sigla em inglês), aprovado pelo Parlamento Europeu em abril de 2016, dispõe que "*os Estados-membros deverão instituir uma ou mais autoridades públicas independentes com o propósito de fiscalizar a observância deste regulamento*". Também prevê que os membros dessas autoridades "*devem agir com total independência no exercício de suas atribuições [...] e não devem estar sujeitos a influências externas, diretas ou indiretas, nem devem solicitar ou receber instruções de outras autoridades.*

No âmbito da OCDE, diversos países optaram pela criação de entidades independentes vocacionadas a apoiar o Estado no gerenciamento de informações pessoais. Nesse modelo, compete a estas entidades a tarefa de construir parâmetros éticos e procedimentos qualificados para o tratamento de dados do cidadão. (OCDE. **The Path to Becoming a Data-Driven Public Sector**. OECD Publishing: Paris, 2019, p. 113).

Coube a cada ente nacional, no exercício de sua soberania, esculpir o arquétipo legal das agências responsáveis pelo controle de atividades potencialmente lesivas ao direito de privacidade. A experiência internacional sinaliza, contudo, um ponto de confluência na legislação dos países democráticos: há uma invariável preocupação de instituir as autoridades nacionais a partir de perfil institucional autônomo, que seja capaz de assegurar o exercício da função de controle com total independência.

Estudo conduzido por **Graham Greenleaf**, a respeito do regime de proteção de dados de 132 países, comprovou que a esmagadora maioria das nações criou agências independentes para fiscalização do tratamento de dados pessoais. Dentro do universo de países analisados, apenas 14 não seguiram esse modelo, relegando a atividade de controle para entidades subordinadas ao governo. Isso, segundo o autor, seria motivo de grande desonra para os integrantes dessa minoria (GREENLEAF, Graham. **Global Data Privacy 2019: DPAS, PEAS and their networks: 158 Privacy Laws & Business International Report**, 2019, pp, 11-14).

Em Portugal, a Lei 58, de 8 de agosto de 2019, assegurou a execução, na ordem jurídica interna, do Regulamento Geral sobre Proteção de Dados (GPDR). Paralelamente ao reconhecimento do direito fundamental à proteção de dados pessoais, o legislador português instituiu a Comissão Nacional de Proteção de Dados (CNPD) como "*entidade administrativa independente, com personalidade jurídica de direito público e poderes de autoridade, dotada de autonomia administrativa e financeira, que funciona junto à Assembleia da República*". Em homenagem à independência da CNPD, a lei lhe atribuiu a seguinte composição multissetorial: (a) três membros eleitos pela Assembleia da República; (b) dois membros indicados pelo Governo; (c) um magistrado indicado pelo Conselho Superior da Magistratura; e d) um membro do *Parquet* designado pelo Conselho Superior do Ministério Público.

No Canadá, o *Privacy Act* de 1985 atribuiu essas atividades a uma autoridade independente denominada *Privacy Commissioner*, indicada pelo Governador-geral (*Governor in Council*), após consulta de todos os

líderes partidários com representação no Parlamento. Após a indicação formal, o nome proposto deve ainda ser aprovado em resolução das duas Casas do Congresso Nacional.

Nos Estados Unidos da América, o Estado da Califórnia editou legislação específica sobre privacidade, intitulada *California Consumer Privacy Act* (CCPA). À semelhança do regulamento europeu, esse moderno diploma legislativo previu que as normas e princípios nele reconhecidos seriam fiscalizados por uma agência independente, composta por (a) um membro indicado pelo Governador; (b) um membro indicado pelo Procurador-Geral; (c) e dois membros indicados pelo Parlamento. Em todos os casos, o CCPA exige que os indicados tenham vasta experiência nas áreas de privacidade, tecnologia e direitos do consumidor.

Na Nova Zelândia, o governo reuniu, no âmbito do Poder Executivo, um Grupo de Aconselhamento Ético para o tratamento de dados pessoais (*Data Ethics Advisory Group*). A esse respeito, é fundamental destacar que, não obstante se trate de órgão de caráter interno, o governo estabeleceu procedimento seletivo público (*expression of interest process*) para escolha dos membros do colegiado, exigindo ainda que os candidatos comprovassem notório conhecimento nas áreas de privacidade, direitos humanos, ética, tecnologia e políticas públicas (https://www.stats.govt.nz/news/stats-nz-convenes-data-ethics-advisory-group).

O exame dos modelos adotados pelas nações democráticas, especialmente pela perspectiva do arquétipo legal das autoridades públicas de controle, revela uma correlação necessária entre a previsão de mecanismos capazes de garantir independência a essas entidades e a efetiva defesa do direito de proteção de dados pessoais.

Nesse sentido, a experiência internacional é capaz de demonstrar que a tutela efetiva do direito à privacidade depende da correta calibragem do perfil institucional dos órgãos responsáveis pela regulamentação, controle e monitoramento de atividades de tratamento de dados pessoais. Assim, é fundamental reconhecer a necessidade de

estruturar essas entidades a partir de uma composição plural e democrática, aberta, em alguma medida, a constante diálogo com a sociedade civil.

No âmbito interno, esse modelo tem sido reproduzido nas legislações setoriais aprovadas pelo Congresso Nacional. É o que ocorreu, por exemplo, com a instituição da Autoridade Nacional de Proteção de Dados (ANPD), composta fundamentalmente por 5 diretores escolhidos pelo Presidente da República e por ele nomeados, após aprovação do Senado Federal. Adicionalmente, a lei exigiu que os membros tenham reputação ilibada, nível superior de educação e elevado conceito no campo de especialidade dos cargos pretendidos**.** Estabeleceu, por fim, mandato de 4 anos para os diretores, que somente perderão seus cargos em virtude de renúncia, condenação judicial transitada em julgado ou pena de demissão decorrente de processo disciplinar (arts. 55-D e 55-E da Lei 13.709/18).

Da mesma forma, a Lei 13.444/17, que dispõe sobre a Identificação Civil Nacional (ICN), instituiu Comitê Gestor do programa, cabendo-lhe, entre outras atribuições, orientar a implementação da interoperabilidade entre a base de dados biométricos da Justiça Eleitoral e os bancos de dados administrados pelo Poder Executivo. Ante a sensibilidade da matéria, o Congresso Nacional atribuiu semblante multissetorial ao Comitê Gestor da ICN, composto por: (a) três representantes do Poder Executivo; (b) três representantes do Tribunal Superior Eleitoral; (c) um representante da Câmara dos Deputados; (d) um representante do Senado Federal; e (e) um representante do Conselho Nacional de Justiça (art. 5º).

Na contramão da experiência internacional e das legislações setoriais aprovadas pelo Congresso Nacional, o Decreto 10.046/19 atribuiu ao Comitê Central de Governança de Dados uma estrutura hermética, ocupada exclusivamente por representantes da Administração Pública federal, designadamente servidores do Ministério da Economia, da Presidência da República, da Controladoria-Geral da União, da Advocacia-Geral da União e do

Instituto Nacional do Seguro Social (art. 22).

Cuida-se, a rigor, de instituição com **perfil insular, hostil a qualquer proposta de abertura democrática e de pluralização do debate** e, nessa medida, fechada à participação de representantes oriundos de outras instituições republicanas e de entidades da sociedade civil.

A falta de alinhamento do ato editado pelo Chefe do Poder Executivo com as boas práticas observadas nas nações democráticas requer atenção do Tribunal. Longe de um mero preciosismo acadêmico, a particular arquitetura institucional introduzida pelo regulamento produz efeitos transversais na ordem jurídico-constitucional, podendo acarretar um autêntico desmonte dos pilares estruturantes da LGPD e, no limite, comprometer a própria eficácia do direito fundamental à proteção de dados pessoais.

As distorções identificadas na composição do Comitê Central de Governança de Dados oferecem, ainda, grave risco de comprometimento da imagem do país no plano externo, podendo, em certa medida, ameaçar pretensões deduzidas pelo Estado brasileiro de ingresso em entidades internacionais relevantes, como a Organização para a Cooperação e Desenvolvimento Econômico – OCDE.

Como se sabe, em janeiro de 2022, o governo brasileiro iniciou tratativas formais para ingresso nesse importante organismo de cooperação multilateral. No curso do processo de adesão, o país será avaliado a respeito da adequação de sua legislação, instituições e práticas aos padrões defendidos pela OCDE em diversos setores, como meio ambiente, saúde, responsabilidade fiscal, sistema tributário e proteção da concorrência e do consumidor.

Não há dúvidas, pois, que, ao longo dos próximos meses, o Estado brasileiro será rigorosamente escrutinado acerca de sua política de privacidade de dados, seja no que diz respeito à existência de instituições capazes de responder diligentemente contra ameaças de malversação dos princípios estruturantes da LGPD, seja no que concerne à compatibilidade do sistema doméstico às normas, aos padrões e aos valores compartilhados pelas nações democráticas.

A propósito do assunto, não se pode perder de vista a advertência feita por **Fabrício Bertini Pasquot Polido**, em artigo publicado no site CONJUR (**O ingresso do Brasil na OCDE e padrões em matéria digital**, Revista Consultor Jurídico, publicado em 7 de março de 2022, disponível em <www.conjur.com.br>). Destaco:

> Além desses objetivos, a OCDE prioriza iniciativas que estejam diretamente atreladas ao livre fluxo de dados e confiança digital. **Não basta a existência de uma Lei Geral de Proteção de Dados – a LGPD – e uma Autoridade Nacional de Proteção de Dados no caso brasileiro, mas antes a consolidação de um desenho institucional dotado de efetividade e autonomia quanto à formulação de políticas e aplicação de decisões, além de princípios de transparência na composição de conselhos políticos.** Práticas sólidas de cooperação digital por parte do Estado brasileiro também serão escrutinadas à luz das diretrizes mais recentes da organização, como os princípios OCDE sobre Inteligência Artificial e objetivos de promoção do livre fluxo de dados com confiança e Princípios de Alto-Nível relativos ao Acesso Confiável de Governos a Dados Pessoais. Membros da OCDE, como na pretendida acessão do Estado brasileiro à organização, devem **assegurar que padrões adequados de privacidade de dados estejam comprovados tecnicamente, com leis e regulamentos que estabelecem regras relativas às garantias de segurança e confiança de usuários de internet e consumidores digitais, além do combate à desinformação e promoção de princípios democráticos e dos direitos humanos associados às operações digitais.**

O perfil orgânico estabelecido pelo decreto se torna ainda mais grave quando constatada a extensão e a relevância das funções desempenhadas pelo Comitê Central de Governança de Dados. Nos termos do art. 21 do Decreto 10.046/2019, compete ao órgão: a) expedir regulamentos para disciplinar a forma, o alcance e os limites inerentes ao compartilhamento

de dados pelos órgãos integrantes da Administração Pública federal; b) deliberar sobre orientações e diretrizes para categorização do compartilhamento amplo, restrito e específico, especialmente à luz da LGPD; c) dispor sobre orientações e diretrizes para acesso de órgãos públicos ao Cadastro Base do Cidadão; d) escolher as bases temáticas que serão integradas ao Cadastro Base do Cidadão; e e) dispor sobre a inclusão, nessa base integradora, de novos dados provenientes das bases temáticas administradas pelos órgãos federais.

Dada a relevância e a sensibilidade da sua missão institucional, é inequívoco que o Comitê Central de Governança de Dados ocupa posição de centralidade no regime constitucional de proteção da privacidade. Cuida-se de entidade que atua em articulação direta com a Autoridade Nacional de Proteção de Dados, desempenhando atribuições que dialogam intimamente com as regras e princípios instituídos pela LGPD, sobretudo no que diz respeito à preservação da privacidade dos usuários de serviços públicos federais.

Essas premissas conduzem à conclusão de que a arquitetura institucional atualmente conferida ao Comitê Central de Governança de Dados **desarticula um mecanismo que é fundamental para o fortalecimento das salvaguardas previstas na LGPD**, no caso, a independência dos órgãos vocacionados ao controle das atividades de tratamento de dados pessoais.

Não bastasse isso, a forma de indicação dos membros desse órgão vai de encontro ao modelo seguido pelas nações democráticas e pelo próprio legislador brasileiro, interditando a participação democrática e a pluralização do debate no âmbito da entidade que estabelece os limites, a extensão e as condições de acesso ao Cadastro Base do Cidadão, seguramente a maior base de dados pessoais existente no território nacional.

A respeito da eficácia objetiva do direito à autodeterminação informativa, **Ingo Wolfgang Sarlet** leciona que *outra importante função atribuída aos direitos fundamentais e desenvolvida com base na existência de um dever geral de efetivação atribuído ao Estado, por sua vez agregado à perspectiva*

*objetiva dos direitos fundamentais, diz com o reconhecimento de deveres de proteção (*schutzpflichten*) do Estado, no sentido de que a este incumbe zelar, inclusive preventivamente, pela proteção dos direitos fundamentais dos indivíduos (...)".* (SARLET, Ingo Wolfgang. **Proteção de Dados Pessoais e deveres de proteção estatais**, Revista Consultor Jurídico, publicado em 27 de agosto de 2021, disponível em <www.conjur.com.br>)

Prossegue o autor afirmando que a tutela do direito à autodeterminação informativa "*depende de estruturas organizacionais e de procedimentos adequados*" que sejam capazes de assegurar, com o maior nível possível de eficácia, a tutela dos valores éticos que orbitam a atual ordem constitucional. Por esse motivo, haveria "*íntima vinculação entre direitos fundamentais, organização e procedimento, no sentido de que os direitos fundamentais são, ao mesmo tempo e de certa forma, dependentes da organização e do procedimento (no mínimo, sofrem uma influência por parte destes), mas simultaneamente também atuam sobre o direito procedimental e as estruturas organizacionais".*

No âmbito acadêmico, já tive a oportunidade de afirmar que "*importante consequência da dimensão objetiva dos direitos fundamentais está em ensejar um dever de proteção pelo Estado dos direitos fundamentais contra agressões dos próprios Poderes Públicos, provindas de particulares ou de outros Estados*". Todavia, ressaltei que não existe "*ordinariamente um dever específico de agir por parte do Estado, uma vez que os Poderes Públicos gozam de discricionariedade para escolher uma das diferentes opções de ação que se lhes abrem, levando em conta os meios que estejam disponíveis, as colisões de direitos e interesses envolvidos e a sua escala de prioridades políticas*". (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de Direito Constitucional,** 14ª edição, São Paulo, Saraiva, 2019, p. 169)

Dessa forma, considerando que o Comitê Central de Governança de Dados é composto única e exclusivamente por representantes do Poder Executivo, e que seus membros não gozam de qualquer garantia contra influências indevidas, entendo que a estrutura organizacional prevista no art. 22 do Decreto 10.046/19 afronta o regime de proteção de dados instituído pela atual ordem constitucional.

Convém ressaltar, todavia, que a invalidação, *tout court*, do dispositivo impugnado acarretaria uma situação ainda mais nociva para a tutela da privacidade dos usuários de serviços públicos, desmantelando a entidade responsável pelo estabelecimento de limites ao compartilhamento de dados entre órgãos da Administração Pública federal.

Ante o risco de desestabilização do sistema, considero prudente reconhecer efeitos prospectivos à declaração de inconstitucionalidade, preservando a atual estrutura orgânica do Comitê Central de Governança de Dados pelo **prazo de 60 dias, a contar da data de publicação da ata de julgamento**. Assim, ao modular os efeitos da decisão, o Tribunal garantirá ao Presidente da República prazo hábil para a superação do modelo orgânico declarado inconstitucional, de modo a resgatar a trajetória de fortalecimento dos mecanismos de proteção de dados pessoais.

Trata-se, a meu ver, de solução conciliatória, que permite ao Tribunal atuar na defesa de direitos negligenciados pelo Estado, sem, contudo, invadir o domínio dos representantes democraticamente eleitos ou assumir compromisso com a conformação da fisionomia de órgãos integrantes do Poder Executivo.

2.7 - Consequências do desrespeito ao regime de proteção de dados pessoais. Surgimento de pretensões materiais e responsabilização do agente público infrator.

A partir da inclusão do direito de proteção de dados pessoais no catálogo de direitos fundamentais, põe-se em perspectiva a questão relativa à responsabilização de agentes públicos pelo descumprimento do dever de tutela previsto no art. 5º, inciso LXXIX, da Constituição Federal.

Trata-se de um debate que assume substancial relevância no âmbito do tratamento de dados por órgãos estatais, na medida em que, dada a colossal extensão dos dados coletados pelo Estado, exsurgem riscos de abusos na utilização dos dados pessoais ou, em caso de omissão ou

desídia do gestor público, de graves incidentes de segurança.

Assim sendo, deixando de lado qualquer pretensão de esgotamento da matéria, o que demandaria uma análise abrangente do ordenamento jurídico brasileiro – algo incompatível com o objeto da demanda – passo a discorrer brevemente sobre as consequências jurídicas do descumprimento do direito fundamental à proteção de dados pessoais.

Sobre o ponto, há consenso na doutrina acerca das consequências imediatas que exsurgem quando levada a efeito uma ingerência (injustificada) no âmbito de proteção de um direito fundamental (SCHLINK, Bernard; PIEROTH, Bodo. **Direitos Fundamentais**. 2ª ed. Saraiva: São Paulo, 2019, p. 124).

Nas palavras de **Ingo Wolfgang Sarlet:**

> "*quando nos referimos aos direitos fundamentais como direitos subjetivos, temos em mente a noção de que ao titular de um direito fundamental é aberta a possibilidade de* ***impor judicialmente seus interesses juridicamente tutelados*** *perante o destinatário*". (...) "*a noção de uma perspectiva subjetiva dos direitos fundamentais engloba a possibilidade de o titular do direito fazer valer judicialmente os poderes, as liberdades ou mesmo o direito de ação ou às ações negativas ou positivas que lhe foram outorgadas pela norma consagradora do direito fundamental em questão* (...)." (SARLET, Ingo Wolfgang. **Curso de Direito Constitucional.** 10ª edição, São Paulo, Saraiva, 2021, pp. 352-353)

Nesse mesmo sentido, o reconhecimento de um direito subjetivo de envergadura constitucional, de acordo com a formulação de **Vieira de Andrade**, está atrelado "*à proteção de uma determinada esfera de autorregulamentação ou de um espaço de decisão individual; tal como é associado a um certo* ***poder de exigir ou pretender comportamentos ou de produzir autonomamente efeitos jurídicos***". (VIEIRA DE ANDRADE. **Os direitos fundamentais na Constituição portuguesa de 1976.** Coimbra: Almedina, 1987, p. 163).

Considerando que o âmbito de proteção do direito à proteção de

dados é instituído, em larga medida, pela atribuição legiferante do Legislador, convém consignar, pelos riscos suscitados pela matéria, que **a violação ao direito de proteção de dados pessoais gera, em favor do cidadão, pretensão de direito material, que por seu turno faculta o exercício do direito de ação**.

Faço, aqui, especial referência ao surgimento da (i) **pretensão reparatória civil**, exercida de acordo com a lógica e as disposições do direito privado; (ii) da **pretensão punitiva disciplinar**, um poder-dever de titularidade da Administração, proveniente dos estatutos dos servidores públicos federais, estaduais, distritais e municipais; e (iii) da **pretensão punitiva**, de caráter eminentemente repressivo, prevista na Lei de Improbidade Administrativa.

Atualmente, diante da clareza do art. 42 da LGPD, há um certo consenso acerca da necessidade de reparação dos danos causados em decorrência do tratamento de dados pessoais. A esse respeito, dispõe a lei que *o controlador ou operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.*

Trata-se de regra evidentemente aplicável ao âmbito do Poder Público, com as devidas adaptações. São pertinentes, a esse respeito, as considerações feitas pelo Supremo Tribunal Federal no julgamento do **tema 940 da repercussão geral**, cujo paradigma é o **RE 1.027.633, de relatoria do EMINENTE MINISTRO MARCO AURÉLIO**, em que se fixou o entendimento de que a ação por danos causados por agente público deve ser ajuizada contra o Estado, a quem compete, posteriormente, exercer o direito de regresso contra o responsável, se identificada conduta culposa ou dolosa.

Assim sendo, o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais (ingerência) importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os

servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa.

Em relação às **pretensões repressivas** e **disciplinares**, há que se ter em mente que, insisto, o compartilhamento de dados entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco 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*".

Dessa forma, **deve-se ter presente que a transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo**, **importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92**, sem prejuízo da incidência de outras tipificações legais, a depender das particularidades do caso concreto.

Assinalo também quanto à possibilidade de responsabilização disciplinar dos servidores públicos pela malversação das informações pessoais, conforme previsto no respectivo estatuto funcional.

Adotados os delineamentos acima expostos, tenho que este Supremo Tribunal Federal fomentará o espraiamento de uma cultura institucional de proteção de dados pessoais no interior dos órgãos administrativos para, com isso, impedir, ou ao menos minimizar, possíveis violações ao direito constitucional à proteção de dados.

III – Conclusão

Ante o exposto, voto no sentido de conhecer a ação direta e a arguição de descumprimento de preceito fundamental e, julgando parcialmente procedentes os pedidos, confiro interpretação conforme ao Decreto 10.046/2019, traduzida nos seguintes termos:

1. O compartilhamento de **dados pessoais** entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de **propósitos legítimos, específicos e explícitos** para o tratamento de dados (art. 6º, inciso I, da Lei 13.709/2018); b) **compatibilidade** do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao **mínimo necessário** para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público.

2. O compartilhamento de **dados pessoais** entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental **compartilha ou tem acesso** a banco 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*".

3. O acesso de órgãos e entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao atendimento integral das diretrizes acima arroladas, cabendo ao Comitê Central de Governança de Dados, no exercício das competências aludidas nos arts. 21, incisos VI, VII e VIII do Decreto 10.046/2019:

> 3.1. prever mecanismos rigorosos de controle de acesso ao Cadastro Base do Cidadão, o qual será limitado a órgãos e entidades que comprovarem **real necessidade** de acesso aos dados pessoais nele reunidos. Nesse sentido, a permissão de acesso somente poderá ser concedida para o alcance de propósitos legítimos, específicos e explícitos, sendo limitada a informações que sejam indispensáveis ao atendimento do interesse público, nos termos do art. 7º,

inciso III, e art. 23, caput e inciso I, da Lei 13.709/2018;

3.2. justificar prévia e minudentemente, à luz dos postulados da proporcionalidade, da razoabilidade e dos princípios gerais de proteção da LGPD, tanto a necessidade de inclusão de novos dados pessoais na base integradora (art. 21, inciso VII) como a escolha das bases temáticas que comporão o Cadastro Base do Cidadão (art. 21, inciso VIII).

3.3. instituir medidas de segurança compatíveis com os princípios de proteção da LGPD, em especial a criação de sistema eletrônico de registro de acesso, para efeito de responsabilização em caso de abuso.

4. O compartilhamento de **informações pessoais em atividades de inteligência** observará o disposto em legislação específica e os parâmetros fixados no julgamento da **ADI 6.529, Rel. Min. Cármen Lúcia**, quais sejam: (i) adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; (ii) instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; (iii) utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abuso; e (iv) observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal.

5. O tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de culpa ou dolo.

6. A transgressão dolosa ao dever de publicidade

> estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/92, sem prejuízo da aplicação das sanções disciplinares previstas nos estatutos dos servidores públicos federais, municipais e estaduais.

Voto, ainda, no sentido de **declarar, com efeito *pro futuro*, a inconstitucionalidade** do art. 22 do Decreto 10.046/19, preservando a atual estrutura do Comitê Central de Governança de Dados pelo prazo de 60 dias, a contar da data de publicação da ata de julgamento, a fim de garantir ao Chefe do Poder Executivo prazo hábil para (i) **atribuir ao órgão um perfil independente e plural, aberto à participação efetiva de representantes de outras instituições democráticas**; e (ii) **conferir aos seus integrantes garantias mínimas contra influências indevidas.**

É como voto.