

MEDIDA CAUTELAR NA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 695 DISTRITO FEDERAL

RELATOR : **MIN. GILMAR MENDES**
REQTE.(S) : **PARTIDO SOCIALISTA BRASILEIRO - PSB**
ADV.(A/S) : **IVO DA MOTTA AZEVEDO CORREA**
INTDO.(A/S) : **UNIÃO**
PROC.(A/S)(ES) : **ADVOGADO-GERAL DA UNIÃO**
AM. CURIAE. : **LABORATORIO DE POLITICAS PUBLICAS E INTERNET LAPIN**
ADV.(A/S) : **HENRIQUE BAWDEN SILVERIO DE CASTRO**

O SENHOR MINISTRO GILMAR MENDES (RELATOR): Trata-se de Arguição de Descumprimento de Preceito Fundamental (ADPF), com pedido de liminar, ajuizada pelo Partido Socialista Brasileiro (PSB), a fim de que seja reconhecida e sanada grave lesão a preceitos fundamentais praticada pelo Poder Público, em razão de “compartilhamento de dados pessoais (...) pelo Serviço Federal de processamento de Dados (SERPRO) à Agência Brasileira de Inteligência (ABIN), com suposto lastro normativo no Decreto nº. 10.046, de 9 de outubro de 2019” (eDOC 1, p. 2).

Narra o requerente que, “Em 6 de junho de 2020, o site jornalístico “The Intercept” noticiou que ABIN e SERPRO estabeleceram tratativas visando ao compartilhamento de dados dos mais de 76 milhões de brasileiros que possuem a Carteira Nacional de Habilitação – CNH1 (o equivalente a 36% da população total do país), originalmente coletados e armazenados pelo do Departamento Nacional de Trânsito (DENATRAN)” (eDOC 1, p. 3), tendo ambas as instituições confirmado a informação e lastreado a conduta sob os preceitos do Decreto 10.046/2019.

Sustenta, em síntese, que o ato do Poder Público federal “(i) viola os preceitos fundamentais da proteção da privacidade, bem como sua consequente garantia de proteção dos dados pessoais e de autodeterminação informativa dos cidadãos brasileiros (art. 5º, incisos X e XII da CF/88) (...), (ii) não passa por crivo de proporcionalidade ou de razoabilidade e (iii) nem possui base normativa que eventualmente lhe dê guarida, (...) (iv) põe em risco o basilar princípio democrático, fundante de nossa ordem constitucional, visto haver risco de vigilância massiva

ADPF 695 MC / DF

sem controle de cidadãos e cidadãos sem qualquer envolvimento com ações ou práticas ilegais (eDOC 1, p. 9).

Aduz que “a transferência massiva e indiscriminada dos dados pessoais de todos os portadores de CNH no país para a Agência Brasileira de Inteligência” (eDOC 1, p. 14) viola os direitos fundamentais à privacidade, à proteção de dados pessoais e à autodeterminação informativa, na medida em que “está sendo operacionalizada sem transparência e à revelia dos titulares dos dados, que não receberam qualquer informação acerca desse compartilhamento, nem qualquer esclarecimento sobre o tratamento a ser realizado pela ABIN. (...) [subvertendo-se] a finalidade para a qual aqueles dados pessoais foram inicialmente coletados, destinando-os a um órgão e a um propósito inteiramente incompatíveis com a finalidade original” (eDOC 1, p. 14). Confronta, nesse ínterim, os princípios da finalidade, da transparência, da adequação e da necessidade, consagrados na Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

Defende a ausência de proporcionalidade e de razoabilidade na medida, posto que “as atividades de inteligência da ABIN podem ser realizadas de maneira menos gravosa ou onerosa a direitos fundamentais, sem que se lese, de uma só vez, a proteção de dados pessoais e a autodeterminação informativa de 76 milhões de pessoas” (eDOC 1, p. 19).

Alega que a legislação de regência da ABIN (Lei nº 9.883/1999) “não traz, em nenhuma de suas previsões, autorização específica para que direitos fundamentais como o da privacidade, da intimidade e da autodeterminação informativa possam ser administrativamente violados, afastados ou restringidos em prol do planejamento e da execução de potenciais ações com o vistas a produzir conhecimento e assessorar o Presidente da República” (eDOC 1, p. 22).

No mais, discorre que o Decreto nº 10.046/2019 não autoriza a medida, uma vez que “estabelece limitações relevantes em prol da defesa e da garantia de direitos fundamentais, especialmente quanto à privacidade, intimidade e autodeterminação informativa” (eDOC 1, p. 23).

ADPF 695 MC / DF

Argui que “a medida questionada carrega em si potencial vigilantismo disseminado em nome do combate a ameaças – reais ou ilusórias – internas e externas”, ao passo que “a potencial utilização de elementos da vida privada dos cidadãos para influenciar, por exemplo, sua participação política, são devastadoras à democracia” (eDOC 1, p. 26).

Requer, assim, a concessão de medida cautelar para “(i) impedir ou cessar imediatamente o compartilhamento à ABIN dos dados colhidos pelo DENATRAN e acessados/gerenciados pelo SERPRO; e (ii) determinar que os dados eventualmente já compartilhados sejam imediatamente inutilizados, sob pena de danos irreparáveis aos direitos de milhões de brasileiros, tornando impossível o retorno ao status quo ante” e, ao final, a procedência da ADPF para “afastar definitivamente o compartilhamento de dados sub judice, dando a correta aplicação e proteção aos preceitos fundamentais em questão” (eDOC 1, p. 31).

Convém destacar ainda que, subsidiariamente, o requerente formulou o pedido de que seja dada interpretação conforme à Constituição Federal, a fim de que “(a) que o rol de finalidades exposto no art. 1º do Decreto nº 10.046, de 2019, seja considerado taxativo e exaustivo, de modo que o tratamento se dê apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, à luz do princípio da finalidade que norteia a proteção de dados pessoais constitucionalmente garantida no país; (b) que, diante da interpretação acima, expressamente se afaste da abrangência do referido Decreto a finalidade de atividade de inteligência, visto que não prevista no ato normativo em causa; e, (c) que, à luz do previsto nos incisos I, V e VI do art. 3 do referido Decreto, se garanta expressamente que o compartilhamento de dados pessoais por órgãos e entidades do setor público está expressamente sujeito e vinculado aos princípios que balizam a proteção de dados pessoais no Brasil, expressos no art. 6º da Lei nº 13.709, de 2018, especialmente quanto à finalidade, adequação, necessidade e transparência” (eDOC 1, p. 32).

Em 17.06.2020, solicitei informações, com urgência, às autoridades

ADPF 695 MC / DF

responsáveis pelo ato e citei o Advogado-Geral da União sobre o objeto da presente arguição (eDOC 11).

Em 20.06.2020, a Advocacia-Geral da União prestou informações (eDOC 14), sustentando (i) a ausência de indicação precisa de ato do Poder Público, (ii) a inobservância do requisito da subsidiariedade, (iii) da ausência de interesse de agir e (iv) a ausência dos requisitos necessários à concessão da medida cautelas (*fumus boni iuris* e *periculum in mora*), em manifestação com a seguinte ementa:

“Constitucional. Compartilhamento de dados de portadores de Carteira Nacional de Habilitação pelo SERPRO para a ABIN. Preliminares. Ausência de indicação precisa de ato do Poder Público. Inobservância do requisito da subsidiariedade. Viabilidade de ajuizamento de outras medidas de tutela coletiva de direitos, inclusive o mandado de segurança, para o qual partidos políticos possuem legitimidade, conforme jurisprudência dessa Suprema Corte. Ausência de impugnação de todo o complexo normativo envolvido. Necessidade de prévio exame da Portaria nº 15/2016, do DENATRAN, e de dispositivos da Lei nº 9.883/1999. Mérito. Ausência de *fumus boni iuris*. O ato administrativo questionado encontra lastro normativo no Decreto nº 10.046/2019, estando pautado no princípio da eficiência e de desburocratização nas atividades do Poder Público. Atividade de inteligência constitui política pública, finalidade admitida como legítima para respaldar o compartilhamento de dados entre órgãos e entidades da Administração Pública. Inexistência de violação aos preceitos constitucionais invocados. Essa Suprema Corte já decidiu que a ‘transferência de dados sigilosos de um determinado portador, que tem o dever de sigilo, para outro, que mantém a obrigação de sigilo’ não ofende o direito à intimidade e à privacidade. ADI nº 2859. Ausência de *periculum in mora*. Manifestação pelo não conhecimento da arguição e, quanto ao pedido de medida cautelar, pelo seu indeferimento.” (eDOC 14, p. 1)

ADPF 695 MC / DF

Nessa manifestação (eDOC 14), AGU afirmou que, em 29.11.2019, “a ABIN enviou ao DENATRAN o Ofício nº 269/2019/SPG/ABIN/GSI/PR, através do qual solicitou acesso a bases de dados daquele órgão, com o objetivo de incrementar o exercício de suas atribuições”. Ainda de acordo com a AGU, “após envio da documentação necessária à instrução do pedido, o DENATRAN concedeu à ABIN o Termo de Autorização nº 7/2020 e orientou o órgão receptor a entrar em contato com o SERPRO para a celebração de contrato administrativo, conforme determina o artigo 22 da Portaria DENATRAN nº 15/2016” (eDOC 14, p. 22).

O ente público afirmou ainda que “segundo informações prestadas pela Consultoria Jurídica do Ministério da Infraestrutura, após prévia consulta do DENATRAN, até o momento, ‘não houve a celebração do necessário contrato com o SERPRO para a obtenção dos dados então requeridos’ ”(eDOC 14, p. 23).

Em 22.06.2020, ante à afirmação da AGU de que houve de fato uma tentativa de compartilhamento da base de dados do DENATRAN com a ABIN, requeri a apresentação do feito em mesa para apreciação do requerimento de concessão da medida cautelar pelo Plenário do STF.

Em 22.06.2020, o Laboratório de Políticas Públicas e Internet (LAPIN) requereu o ingresso no feito como *amicus curiae* (eDOC 18).

Em 23.06.2020, às vésperas do julgamento da medida cautelar pelo Plenário do STF, a AGU peticionou nos autos informando que, como consignado em sua manifestação anterior, “a ABIN de fato solicitou acesso à base de dados do DENATRAN, mediante pedido processado conforme à Portaria nº 15/2016/DENATRAN. A requisição que foi deferida na forma do Termo de Autorização nº 7/2020, do DENATRAN, publicado no Diário Oficial da União – DOU Nº 46, Seção 3, de 9 de março de 2020” (eDOC 28).

Todavia, a AGU informou que embora a autorização nem tenha chegado a surtir efeitos práticos, a Secretaria Nacional de Transportes Terrestres, do Ministério da Infraestrutura, diligenciou ativamente pela sua revogação, conforme consta da Nota Técnica nº 626/2020/CGATF-DENATRAN/SNTT. A AGU juntou ainda aos autos documento de

ADPF 695 MC / DF

revogação do Termo de Autorização, devidamente assinado pelo Diretor-Geral do DENATRAN, encaminhado para publicação na Imprensa Oficial (eDOC 29).

Em 24.06.2020, foi publicado em Edição Extra do Diário Oficial da União (DOU) o Aviso de Revogação do Termo de Autorização 7/2020-A.

É o relatório.

1. Das preliminares

Em manifestação (eDOC 14), a Advocacia-Geral da União suscitou preliminares ao mérito, em correspondência aos requisitos do art. 3º da Lei 9.882/1999. No entanto, não percebo pertinência das alegações ao caso, como exponho a seguir.

De início, rechaço o argumento em relação à ausência de indicação precisa de ato do Poder Público, posto que a lesão a preceitos fundamentais por ato concreto do Poder Público – compartilhamento de dados constantes na Carteira Nacional de Habilitação entre o SERPRO e a ABIN – parece suficientemente indicada na peça inicial, sendo comprovada pelos documentos colacionados, que indicam (i) a transmissão da informação por veículo de mídia (eDOC 5) e (ii) a confirmação desta em manifestação das autoridades (eDOCs 6 e 7). 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, de modo que inexistente vício processual.

Como a União, neste ponto, junta aos autos acervo probatório complementar – em especial a Portaria nº 15/2016, do DENATRAN, e o Termo de Autorização nº 07/2020, emitido pelo DENATRAN em favor da ABIN (eDOC 15) –, o cotejo destas provas àquelas colacionadas à exordial será necessário para a apreciação do pleito cautelar.

Afasto, ainda, a alegação preliminar no que diz respeito à ausência de impugnação adequada de todo o complexo normativo em que a medida administrativa está inserida, porquanto, dos documentos já ressaltados e dos fundamentos da exordial, extraem-se os devidos

ADPF 695 MC / DF

parâmetros de constitucionalidade – art. 1º, III, e art. 5º, *caput*, X e XII, do texto constitucional –, bem como o teor de normas infraconstitucionais pertinentes – Lei nº 9.883/1999 e Lei nº 13.709/2018 –, sendo suficientes ao conhecimento da ADPF. Não há, assim, óbice intransponível nesse ponto.

Também não vislumbro a inobservância ao requisito da subsidiariedade *in casu*. Importa destacar, a princípio, que a Lei 9.882/1999 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).

À primeira vista, poderia parecer que, somente na hipótese de absoluta inexistência de qualquer outro meio eficaz a afastar a eventual lesão, poder-se-ia manejar, de forma útil, a arguição de descumprimento de preceito fundamental.

Uma leitura mais cuidadosa há de revelar, porém, que, na análise sobre a eficácia da proteção de preceito fundamental nesse processo, 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 (o que é resultado, inclusive, da legitimação ativa), 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.

A respeito, 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. Nesse sentido, destaco a decisão monocrática do Min. Celso de Mello, na ADPF 126-MC, datada de 19.12.2007:

“O diploma legislativo em questão – tal como tem sido reconhecido por esta Suprema Corte (RTJ, 189/395-397, v. g.) – consagra o princípio da subsidiariedade, que rege a instauração

do processo objetivo de arguição de descumprimento de preceito fundamental, condicionando o ajuizamento dessa especial ação de índole constitucional à ausência de qualquer outro meio processual apto a sanar, de modo eficaz, a situação de lesividade indicada pelo autor: (...) O exame do precedente que venho de referir (RTJ 184/373-374, rel. min. Celso de Mello) revela que o princípio da subsidiariedade não pode – nem deve – ser invocado para impedir o exercício da ação constitucional de arguição de descumprimento de preceito fundamental, eis que esse instrumento está vocacionado a viabilizar, numa dimensão estritamente objetiva, a realização jurisdicional de direitos básicos, de valores essenciais e de preceitos fundamentais contemplados no texto da Constituição da República. (...) **Daí a prudência com que o Supremo Tribunal Federal deve interpretar a regra inscrita no art. 4º, § 1º, da Lei n. 9.882/99, em ordem a permitir que a utilização dessa nova ação constitucional possa efetivamente prevenir ou reparar lesão a preceito fundamental causada por ato do Poder Público. Não é por outra razão que esta Suprema Corte vem entendendo que a invocação do princípio da subsidiariedade, para não conflitar com o caráter objetivo de que se reveste a arguição de descumprimento de preceito fundamental, supõe a impossibilidade de utilização, em cada caso, dos demais instrumentos de controle normativo abstrato:** (...) A pretensão ora deduzida nesta sede processual, que tem por objeto normas legais de caráter pré-constitucional, exatamente por se revelar insuscetível de conhecimento em sede de ação direta de inconstitucionalidade (RTJ 145/339, Rel. Min. Celso de Mello – RTJ, 169/763, Rel. Min. Paulo Brossard – ADI 129/SP, Rel. p/ o acórdão Min. Celso de Mello, v. g.), não encontra obstáculo na regra inscrita no art. 4º, § 1º, da Lei n. 9.882/99, o que permite – satisfeita a exigência imposta pelo postulado da subsidiariedade – a instauração deste processo objetivo de controle normativo concentrado. Reconheço admissível, pois, sob a perspectiva do postulado da subsidiariedade, a utilização do instrumento processual da arguição de descumprimento de

ADPF 695 MC / DF

preceito fundamental” (Grifei)

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 arguição tem por objeto imediato ação administrativa supostamente lastreada no Decreto Federal nº 10.046/2019, na Portaria nº 15/2016 do DENATRAN e no Termo de Autorização nº 07/2020, emitido pelo DENATRAN em favor da ABIN.

A potencial lesão a preceitos fundamentais esgota-se tão logo haja o compartilhamento indevido de dados pessoais pelas autoridades do Poder Público. Dessa forma, mesmo que, em tese, cabível o acesso à jurisdição ordinária, não há tempo hábil para uma resposta jurisdicional voltada para o caso concreto, ainda que liminar.

Transparente 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, em destaque, o caráter marcadamente objetivo que se 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 medida em que, recentemente, esta Suprema Corte reconheceu a proteção de dados pessoais como direito fundamental autônomo (julgamento conjunto das ADI 6387, 6388, 6389, 6390 e 6393, Rel. Min. Rosa Weber).

ADPF 695 MC / DF

Por tudo, a arguição de descumprimento de preceito fundamental não apresenta óbices preliminares intransponíveis a ensejar a inépcia ou o indeferimento liminar (art. 4º da Lei 9.882/1999).

2 – Do mérito

A despeito de a União ter suscitado, às vésperas da apreciação da Medida Cautelar nesta ADPF pelo plenário do STF, alegação de perda de objeto da presente ação, dada a complexidade da matéria e a relevância dos fundamentos das decisões do STF em sede de controle abstrato de constitucionalidade, passo ao exame da verossimilhança do direito alegado na inicial.

Considero oportuno fazer algumas advertências iniciais, dada a complexidade da matéria e a celeridade de processamento da ADPF neste Tribunal.

Em primeiro lugar, é importante situar epistemologicamente que o parâmetro de controle invocado nesta ADPF está relacionado à afirmação do direito à proteção de dados pessoais enquanto categoria autônoma de direito fundamental na ordem constitucional brasileira, especialmente na forma de uma projeção alargada do direito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, consagrado no art. 5º, inciso X, da CF.

A compreensão da forma de incidência desse parâmetro de controle no caso concreto, por sua vez, demanda que se examine como as leis gerais de internet vigentes no nosso país incorporam e reverberam a conformação dessas garantias constitucionais.

Como já tive a oportunidade de ressaltar recentemente em âmbito acadêmico, sob o ponto de vista da chamada teoria do Constitucionalismo Digital, há uma preocupação de que a interpretação de leis como o nosso Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais se oriente por princípios e valores normativos que considerem de forma harmônica os impactos que declarações de direitos, posicionamentos de organizações internacionais e propostas legislativas

ADPF 695 MC / DF

exercem sobre a proteção de direitos fundamentais no ciberespaço.

Um corolário imediato dessa compreensão é o reconhecimento de que as cartas jurídicas de enunciação de direitos dos usuários da internet muitas vezes contêm verdadeiras **escolhas de matriz constitucional** quanto ao tratamento jurídico a ser conferido às relações on-line. (MENDES, Gilmar Ferreira e FERNANDES, Victor Oliveira. **Constitucionalismo Digital e Jurisdição Constitucional: uma agenda de pesquisa para o caso brasileiro**. In: MORAIS, Carlos Blanco de e MENDES, Gilmar Ferreira. Public Governance 4.0. Editora Almedina. *No Prelo*, 2020).

Assim, para análise do presente caso, far-se-á imprescindível o exame atento da legislação aplicável ao tratamento de dados pessoais pelo Poder Público, não para que se faça das legislações infraconstitucionais um parâmetro de controle de constitucionalidade do ato do poder público, mas sim para que os contornos das garantias constitucionais previstas no art. 5º, inciso X, da CF sejam mais bem compreendidas.

Em segundo lugar, é importante esclarecer que também não se discute nesta ADPF a possibilidade de os órgãos do Sistema Brasileiro de Inteligência em geral e a ABIN em especial realizarem tratamentos de dados para suas finalidades legais de inteligência. Essa prerrogativa encontra lastro inquestionável na Lei 9.883/1999, que institui a Política Nacional de Inteligência. O que se impugna nesta ação, por outro lado, é a constitucionalidade de atos concretos do Poder Público que visavam ao compartilhamento de dados constantes da base do DENATRAN – a qual engloba informações de 76 milhões de brasileiros – entre órgãos e entidades que não integram o Sistema Brasileiro de Inteligência e a ABIN. Subsidiariamente, o requerente impugna ainda, de forma abstrata, a constitucionalidade do art. 1º do Decreto 10.046/2019.

Feitos esses esclarecimentos iniciais, lembre-se que a concessão, pelo STF, de medida cautelar em ação direta de inconstitucionalidade e em ação declaratória de constitucionalidade tem-se mostrado instrumento apto à proteção da ordem constitucional, como demonstra a

ADPF 695 MC / DF

jurisprudência da Corte. Como é cediço, a medida cautelar em ação direta depende do atendimento de dois pressupostos, que são: (1) a verossimilhança do direito e (2) o perigo da demora.

Verifico, na hipótese, embora esteja presente o requisito da verossimilhança do direito alegado, a apontar uma situação de grave ofensa à ordem constitucional, o perigo da demora relativo especificamente ao pedido de suspensão do ato do poder público materializado no Termo de Autorização 7/2020 foi afastado ante à sua recente revogação (eDOC 28). Passo ao exame destes dois itens.

2.1 – Da verossimilhança do direito alegado

2.1.1 – Direito fundamental à proteção de dados pessoais: evolução histórica

O autor defende que o compartilhamento de dados constantes na carteira nacional de habilitação, possibilitado por tratativas entre o SERPRO e a ABIN, seria incompatível com os preceitos fundamentais contidos nos artigos 1º, inciso III; e 5º, *caput* e incisos X, XII e LXXII, da Constituição Federal.

A adequada compreensão do parâmetro de controle invocado perpassa o inevitável aprofundamento de afirmação da autonomia do direito fundamental à proteção de dados pessoais como categoria dentro do rol dos direitos fundamentais.

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, colmatando-se o núcleo da proteção jurídica como o 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).

Na doutrina pátria, os 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**. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, p. 430-459, 1993).

O corolário imediato dessa subsunção do direito à privacidade à função negativa de um direito fundamental personalíssimo limitou o reconhecimento da proteção constitucional ao sigilo (art. 5º, inciso XII) ao conteúdo das comunicações. Tal abordagem formalista influenciou sobremaneira a jurisprudência do Supremo Tribunal Federal na década passada, sobretudo no julgamento do Mandado de Segurança 21.729/DF e no julgamento do Recurso Extraordinário 418.416-8/SC.

Neste último caso, o Tribunal negou que as informações contidas nesses registros estariam acobertadas pelo direito à privacidade, reproduzindo mais uma vez a fórmula do professor **Ferraz Júnior**, nos termos do voto do Ministro **Sepúlveda Pertence**, relator, para quem não teria havido violação ao art. 5º, inciso XII, da Constituição, uma vez que não teria ocorrido quebra de sigilo das comunicações de dados (interceptação das comunicações), mas tão somente apreensão de base física na qual se encontravam os dados. (RE 418.416, Rel. Min. Sepúlveda

ADPF 695 MC / DF

Pertence, Tribunal Pleno, DJ 19.12.2006).

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 verdadeira mutação jurídica do sentido e do alcance do direito à privacidade. Nas palavras de **Stefano Rodotà**, nas últimas décadas, 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** (DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Renovar: Rio de Janeiro, 2006). 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, em última análise, inviabilizariam o livre desenvolvimento da sua personalidade.

A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo

ADPF 695 MC / DF

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, op. cit., p. 141-142).

O marco identificador da reconceptualização do direito à privacidade coincide com o desenvolvimento jurisprudencial do conceito de autodeterminação informacional (*die informationelle Selbstbestimmung*) pelo Tribunal Constitucional Alemão em 1983.

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 (*Volkszählungsgesetz*), 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 ampliada 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

ADPF 695 MC / DF

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, op. cit., 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 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 um 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

ADPF 695 MC / DF

o direito de escolher livremente o seu modo de vida" (tradução livre) (RODOTÀ, Stefano. **In diritto di avere**. Roma: Laterza, 2012, p. 321).

A rigor, 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 inclusive 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 (Lei 13.709/2018). Este último diploma assenta de maneira clara que “a disciplina da proteção de dados pessoais tem como fundamentos o respeito à privacidade e a autodeterminação informativa”(art. 2º, incisos I e II).

A abertura do texto constitucional ao reconhecimento da autonomia do direito fundamental à proteção de dados pode ser identificada na própria jurisprudência desta Corte. Ao apreciar o tema 582, da repercussão geral (Recurso Extraordinário 673.707, Rel. Min. Luiz Fux), o Plenário do STF entendeu pelo cabimento de *habeas data* para fins de acesso a informações incluídas em banco de dados denominado SINCOR – Sistema de Conta-Corrente de Pessoa Jurídica, da Receita Federal (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, julgado em 17.6.2015, DJe 30.9.2015).

Essa orientação se justificou ante o fato de os dados serem entendidos em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto, causando-lhe dano ao seu direito de privacidade. Assim, aos contribuintes foi assegurado constitucionalmente o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o *status* de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente.

Mais recentemente, o STF chancelou a autonomia do direito fundamental à proteção de dados pessoais ao declarar a

ADPF 695 MC / DF

inconstitucionalidade da Medida Provisória 954/2020, que dispunha sobre o compartilhamento de dados de usuários dos serviços de telefonia fixa e móvel de milhões de brasileiros com o IBGE. Embora o acórdão referente ao julgamento ainda esteja pendente de publicação, colhe-se do Informativo 976 do STF:

“O colegiado observou que o único dispositivo da MP 954/2020 a dispor sobre a finalidade e o modo de utilização dos dados objeto da norma é o § 1º do seu art. 2º. E esse limita-se a enunciar que os dados em questão serão utilizados exclusivamente pelo IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares. Não delimita o objeto da estatística a ser produzida, nem a finalidade específica, tampouco sua amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados. O art. 1º, parágrafo único, da MP 954/2020 apenas dispõe que o ato normativo terá aplicação durante a situação de emergência de saúde pública decorrente do Covid-19. Ainda que se possa associar, por inferência, que a estatística a ser produzida tenha relação com a pandemia invocada como justificativa da edição da MP, tal ilação não se extrai de seu texto.

Assim, não emerge da MP 954/2020, nos termos em que posta, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, consideradas a necessidade, a adequação e a proporcionalidade da medida. Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP 954/2020 não oferece condições para avaliação da sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades”.

ADPF 695 MC / DF

Dessa maneira, é sob essa ótica da afirmação da autonomia do direito fundamental à proteção de dados pessoais que deve ser examinada a violação aos preceitos fundamentais na presente ação.

2.1.2 – Autonomia e núcleo essencial do direito fundamental na ordem constitucional brasileira

Essas considerações teóricas sobre o núcleo essencial do direito fundamental à proteção de dados pessoais afiguram-se indispensáveis para o exame do caso concreto. Isso porque **os argumentos sustentados pela União em sua manifestação parecem espelhar justamente a concepção jurídica ultrapassada que ombreia o direito à privacidade ao direito fundamental ao sigilo.**

Não se olvida que o regramento aplicável ao compartilhamento de dados entre o DENATRAN e a ABIN, nos termos da Portaria DENATRAN 15/2016 e do Termo de Autorização 7/2020, de fato contemple o dever de sigilo quanto ao uso das informações referentes aos dados disponibilizados. Nem poderia ser diferente, dado que o manejo de dados pelos servidores públicos em qualquer hipótese se submete à garantia constitucional de sigilo, sendo até mesmo objeto de tutela nas esferas cível, disciplinar administrativa e penal.

Todavia, sob a ótica do direito fundamental à proteção de dados, não é suficiente que o Termo de Autorização 7/2020 estabeleça que os dados repassados a ABIN devem ser protegidos “*sigilo das informações obtidas, não sendo permitido, a qualquer título, ceder a terceiros o direito de acesso*”, tendo limitado, no mais, a disponibilização apenas às “*informações necessárias à execução dos serviços e de sua finalidade*”. Do mesmo modo, a mera referência, na Portaria DENATRAN 15/2016, de que o órgão deve manter o sigilo das informações compartilhadas também pouco acrescenta à discussão aqui colocada.

É claro que a proteção do sigilo em operações como essas é indispensável. Contudo, a autonomia do direito fundamental em jogo na presente ADPF exorbita, em essência, a sua mera equiparação com o

ADPF 695 MC / DF

conteúdo normativo da cláusula de proteção ao sigilo.

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

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

Em uma **dimensão subjetiva**, a proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e, em uma perspectiva objetiva, a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados. (MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 140., p. 176-177).

A partir da tradição norte-americana, também é possível identificar como corolário da dimensão subjetiva do direito à proteção de dados pessoais, a preservação de verdadeiro “devido processo informacional” (*informational due process privacy right*), voltado a conferir ao indivíduo o direito de evitar exposições de seus dados sem possibilidades mínimas de controle, sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios.

Como destacado por Julie E. Cohen: “o caráter autônomo da privacidade sugere uma necessidade de repensar a concepção do devido processo como uma tomada de decisão individualizada. (...) O devido processo na era de computação abrangente deve pressupor limites à personalização nos processos administrativos públicos” (COHEN, Julie E.

What Privacy is For. *Harvard Law Review*, Vol. 126, 2013, p. 1931).

Já em uma **dimensão objetiva**, a afirmação do direito fundamental à proteção de dados pessoais impõe ao legislador um verdadeiro dever de proteção (*Schutzpflicht*) do direito à autodeterminação informacional, o qual deve ser colmatado a partir da previsão de mecanismos institucionais de salvaguarda traduzidos em normas de organização e procedimento (*Recht auf Organisation und Verfahren*) e normas de proteção (*Recht auf Schutz*). Essas normas devem ser positivadas justamente para garantir o controle efetivo e transparente do indivíduo relativamente à circulação dos seus dados, tendo como chave-interpretativa da juridicidade desse controle a noção de consentimento.

Ainda no bojo dessas normas de organização e procedimento, a evolução do regime de proteção de dados no plano transnacional tem convergido no diagnóstico de que o cumprimento eficaz dos limites e finalidades específicas do tratamento de dados invariavelmente perpassa a atribuição dessa função a uma autoridade independente, como disposto no **art. 8º da Carta de Direitos Fundamentais da União Europeia**:

“Art. 8º. da Carta de Direitos Fundamentais. Art. 8o. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. **O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.**”

Como bem destacado pela professora **Indra Spiecker genannt Döhm**: “*um elemento central da proteção por meio do direito procedimental e organizacional é a institucionalização de autoridades de fiscalização independentes nos Estados-Membros (art. 51 e ss. do RGPD)*” (tradução livre) (DÖHMANN, Indra Spiecker genannt. A Proteção de Dados Pessoais sob

ADPF 695 MC / DF

o Regulamento Geral de Proteção de Dados da União Europeia. No prelo).

Sobre esse último ponto, não há como deixar de observar que, no caso brasileiro, malgrado ter transcorrido mais de um ano da promulgação da LGPD, ainda não foram adotadas medidas para instituição da Autoridade Nacional de Proteção de Dados (ANPD).

Nesse contexto, **o que está em jogo na presente ADPF é em que medida o ato do Poder Público aqui impugnado e em especial o Termo de Autorização 7/2020 trazem ou não salvaguardas suficientes para garantir o direito do cidadão de ter o controle sobre a governança dos seus dados.**

Diferentemente do que ocorre com o direito fundamental ao sigilo, a **dimensão subjetiva** do Direito Fundamental à Proteção de Dados Pessoais impõe que o legislador e o Poder Público de modo geral assumam o **ônus de apresentar uma justificativa constitucional para qualquer intervenção que de algum modo afete a autodeterminação informacional.**

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

Assim, no caso em tela, o que está em jogo não é apenas o nível de segurança da informação objeto do compartilhamento entre DENATRAN e ABIN, mas sim **a existência de mecanismos adequados de controle das finalidades desse compartilhamento.** Essa nova abordagem jurídica do direito fundamental à proteção de dados, nesse aspecto, engloba uma **proteção abrangente,** que desloca o eixo da proteção do conteúdo dos dados para as possibilidades e finalidades do seu processamento.

Por essa razão, também parece ser insuficiente o argumento de que o compartilhamento dos dados objeto do Termo de Autorização 7/2020 limitar-se-ia a dados não sensíveis, isto é que não alcançariam as

ADPF 695 MC / DF

informações qualificadas pela Lei 13.709/2018.

Esse argumento também foi sustentado pela União em sua manifestação, no ponto em que asseverou que “o acesso conferido à agência de inteligência, identificado pelo próprio arguente como correspondente aos ‘nomes, filiação, endereços, telefones, dados dos veículos e fotos de todo portador’ (fl. 02 da petição inicial), não abarca elementos sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter sigiloso, filosófico ou político, tampouco dados genéticos, biométricos ou referentes à saúde ou à vida sexual dos indivíduos” (eDOC 14).

A concepção autônoma de um direito fundamental à proteção de dados pessoais enquanto garantia objetiva de governança sobre o controle desses ativos torna secundário – para não dizer irrelevante – a categorização de dados pessoais e dados pessoais sensíveis.

Como bem destacado pela professora **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 dos 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 que quão sensíveis ou íntimos eles são)” (MENDES, Laura Schertel. **Autodeterminação informativa: a história de um conceito. No Prelo**).

Essa abrangência da proteção atribuída ao direito de autodeterminação constitui importante chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais, **o qual não recai propriamente sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros.**

Desse modo, rejeito de plano os argumentos trazidos pela União quanto à alegação de que as normas de proteção ao sigilo previstas no Decreto 10.046/2019 e na Portaria 15/2016 do Denatran seriam, por si só, suficientes para resguardar o direito fundamental à proteção de dados pessoais cuja tutela se busca na presente ADPF.

2.1.3 – Tratamento de dados pessoais pelo Poder Público: princípios constitucionais aplicáveis e rejeição ao isolamento do interesse público

A discussão jurídica travada nesta ADPF assume contornos bem particulares em relação ao debate recentemente enfrentado por esta Corte na análise da ADI 6.389 MC, rel. Min. Rosa Weber. Isso se deve principalmente às complexidades que permeiam o tratamento de dados no âmbito do Poder Público.

É inegável que as relações jurídicas entre o Estado e os cidadãos comportam particularidades que desaconselham um simples traslado do regramento de proteção de dados pessoais nas relações privadas. Isso porque, para além da questão meramente econômica, os dados constituem ativos estratégicos para a gestão pública nas sociedades contemporâneas e, além disso, constituem verdadeiramente pré-condições para o exercício da democracia.

Considerando o interesse público envolvido nas atividades de proteção de dados pessoais pela Administração e o próprio caráter compulsório do relacionamento entre os particulares e o Estado, é possível concluir, como bem destacado pela professora **Miriam Wimmer**, em artigo sobre o tema, que *“o tratamento de dados pessoais pelo Estado é imprescindível para o desempenho do seu mandato constitucional”*. (WIMMER, Miriam. **Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público**. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional. No prelo).

Como ressalta ainda a autora, seria imaginável, 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”

ADPF 695 MC / DF

(ibidem).

Essas questões são ainda mais sensíveis no campo da segurança pública ou no das atividades de inteligência, como se discute nessa ADPF. Isso porque dificilmente faria sentido dizer que, para que um criminoso ou suspeito pudesse ter seus dados tratados pelo Poder Público, seria necessário o pleno consentimento do cidadão. Nesses casos, torna-se de fato discutível em que medida a utilidade pública envolvida no tratamento desses dados pode impor a flexibilização das limitações impostas por uma legislação protetiva.

Sobretudo com o 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 a partir da 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 princípios constitucionais estão em jogo quando se discutem os limites do tratamento de dados pelo Poder Público, tais como o princípio da eficiência da Administração Pública (art. 37, CF). Como destacado pela

própria União em sua manifestação nos autos, sem dúvida o compartilhamento efetivo de dados entre os órgãos e entidades da Administração Federal é exteriorização de uma gestão pública eficiente.

Todavia, diferente do que assevera a AGU nos autos, 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 **Guilian Black** e **Leslie Stevens**, pesquisadores britânicos dedicados a essa temática, “se a privacidade for tratada simplesmente como um direito ou interesse individual, sempre será possível para o setor público controlar dados para suas finalidades públicas, já que isso será sempre reputado como necessário e proporcional” (tradução livre) (BLACK, Gillian e STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest**. Scripted. Vol. 10, n. 1, 2013, p. 95).

Nesse sentido, assentam ainda 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. 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 recentemente passaram a adotar critérios formais, definidos em legislação própria, para proteger os cidadãos no processo de coleta, armazenamento, compartilhamento e

ADPF 695 MC / DF

processamento de dados pelos órgãos do Estado. Em patamares de proteção mais elevado, 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 a 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).

Esses parâmetros apontados pela OCDE parecem estar sendo perseguidos constantemente 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 liderança de uma entidade independente vocacionada a apoiar as entidades governamentais a gerenciar os dados que elas possuem sobre os cidadãos como um ativo estratégico, facilitando o acesso e o compartilhamento de dados a partir de *standarts* 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 de estabelecer guias vinculantes em relação ao próprio Estado, limitando o processamento dos dados dos cidadãos. No Reino Unido, por exemplo, observa-se que em complementação às 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*, o qual determina que cada Ministro competente expeça um código de conduta para compartilhamento de informações dentro de cada uma dessas finalidades legais e ainda o *Data Ethics Framework*, que traz orientações bastante pragmáticas para serem utilizadas no dia a dia

ADPF 695 MC / DF

dos servidores públicos.

Trazendo essas considerações para o caso nacional, mesmo que se entenda que o direito fundamental à proteção de dados pessoais não é absoluto, é inequívoco que se deve buscar uma harmonização dos interesses do Estado tutelados constitucionalmente com os imperativos de proteção de garantias individuais. Sobre esse ponto, destaca-se mais uma vez o escólio de **Miriam Wimmer** no sentido de que:

“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 determina 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 Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). *Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional*. No prelo).

Convém destacar que essa visão de compatibilização dos interesses da Administração Pública com a defesa de garantias individuais na temática da proteção de dados pessoais no Poder Público não é de todo estranha à jurisprudência do STF. Em pelo menos duas ocasiões, o Tribunal impôs limitações a um modelo de fluxo multidirecional e irrestrito do compartilhamento de dados entre órgãos e instituições

públicas.

Destaca-se, nesse sentido, decisão da lavra da então presidente Ministra Cármen Lúcia na Suspensão de Liminar 1.103 MC, em que Sua Excelência determinou que o IBGE se abstinhasse de fornecer ao Ministério Público Federal dados reputados necessários à identificação de 45 (quarenta e cinco) crianças, na área urbana do município de Bauru/SP, desprovidas de registro de nascimento e, por conseguinte, da proteção do Estado e da sociedade. Nessa decisão, a Min. Cármen Lúcia afirmou a necessidade de conciliação dos valores constitucionais em jogo ao pontuar que:

“O dever de sigilo proporciona segurança a quem presta as informações e contribui para a confiabilidade das pesquisas efetuadas. Recepção das normas que estabelecem o sigilo das informações colhidas pelo IBGE (art. 2º, § 2º, do Decreto-lei n. 16111967 e parágrafo único, do art. 1º, da Lei no 5.534/1968) pela Constituição Federal de 1988. IV. Quando princípios fundamentais da Constituição conflitam entre si, a questão deve ser analisada tendo em vista o caso concreto, respeitados os 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”. (SSL 1.103 MC, Rel. Min. Cármen Lúcia, julgado em 5.2.2017, DJe 8.5.2017).

No mesmo sentido, cumpre citar ainda decisão recente de lavra do Ministro Luís Roberto Barroso, nos autos do Mandado de Segurança

ADPF 695 MC / DF

36.150 MC, em que o relator deferiu a cautelar para cassar determinação do Tribunal de Contas da União (TCU), que ordenara ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP a entrega de dados individualizados do Censo Escolar e do ENEM para auditoria do Programa Bolsa Família.

Destaca-se que, nessa decisão, o relator apontou o risco de o tratamento de os dados compartilhados pelo INEP serem submetidos a uma finalidade diversa daquela originalmente declarada no ato da coleta. Desse modo, a decisão do Ministro Luís Roberto Barroso dialoga profundamente com a noção do princípio da finalidade aqui discutida. Destaca-se trecho da decisão nesse sentido:

“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

ADPF 695 MC / DF

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 proteção aos direitos individuais, notadamente com a garantia de autodeterminação informativa espalhada no art. 5º, *caput* e incisos X, XII e LXXII, da Constituição Federal.

2.1.4 – Fundamentos legais e infralegais do tratamento e compartilhamento de dados no Poder Público: o ponto cego do ordenamento jurídico brasileiro

A discussão que se enfrenta nesta ADPF consiste em saber se o compartilhamento de dados entre o DENATRAN e a ABIN, nas condições atuais ainda pouco conhecidas, pode ser considerado um tratamento de dados legítimo do ponto de vista constitucional. Em outras palavras, o que se examina nesta ação é se, sob a ótica do próprio princípio da legalidade, a atuação do Estado para a finalidade posta é compatível com o regime de proteção à privacidade e de proteção de dados pessoais.

A resposta a esse questionamento, todavia, é pouco intuitiva. Isso porque, no ordenamento jurídico pátrio, ainda **há significativos pontos cegos sobre o regime de proteção de dados no que aplicável às relações firmadas com o Poder Público**. Esses pontos cegos nublam os limites da ação estatal e sua colmatação deve ser buscada pelo Poder Legislativo, na linha do que vem sendo realizado por nações democráticas, como já discutido no presente voto.

Examinando-se a legislação aplicável, diagnostica-se que, nos últimos dez anos, foram editados diversos atos normativos que disciplinam o uso compartilhado de dados na Administração Pública Federal, todos eles voltados a impulsionar a desburocratização de procedimentos e o combate a fraudes nos serviços públicos.

Essas alterações recentes, contudo, parecem ter caminhado na contramão do movimento normativo de valorização dos direitos fundamentais na internet nas relações privadas, movimento esse que se

consolidou a nível legal com a edição do Marco Civil da Internet e da Lei Geral de Proteção de Dados.

Atualmente, o tratamento de dados pelo Poder Público é regido sobretudo pela Lei Geral de Proteção de Dados e pelo Decreto 10.046, de 9 de outubro de 2019, que instituiu o chamado Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

No regime da LGPD, não remanescem dúvidas sobre a aplicabilidade dessa lei às relações entre os indivíduos e o Poder Público, já que a sua incidência abrange o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa jurídica de direito público ou privado (art. 1º). **A lei esclarece que ao compartilhado de dados pessoais pelo Poder Público são aplicáveis os mesmos princípios de proteção de dados pessoais, tais como o princípio da finalidade, da adequação, da necessidade e da não discriminação (art. 6º).** Esses princípios espelham, como já destacado, verdadeiros desdobramentos da dimensão subjetiva do direito fundamental à proteção de dados pessoais. Isso ocorre sobretudo em relação ao princípio da finalidade, segundo o qual os dados só podem ser tratados e utilizados pela instância responsável para a finalidade para a qual foram captados.

Diante dessas dificuldades, o grande desafio é saber exatamente como esse regramento proto-constitucional é aplicável ao tratamento de dados pelo Poder Público. Nesse ponto, a doutrina sustenta que, à semelhança do que ocorre com a Lei Europeia (GDPR), a LGPD parece ter dado preferência a um regime de bases legais específicas para as relações público-privadas.

Dentre essas bases legais específicas, a LGPD estabelece duas matrizes centrais: o tratamento de dados (i) para a execução de políticas públicas e (ii) para a execução de competências legais do serviço público. Essas bases legais podem ser extraídas da literalidade do art. 7, inciso III, art. 11, inciso II, e art. 26 da lei:

“Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

(...) III - pela administração pública, para o tratamento e

ADPF 695 MC / DF

uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

(...)

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

(...) II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; (...)

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.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

I - em casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na [Lei nº Lei nº Lei nº Lei nº Lei nº Lei nº Lei nº Lei nº Lei nº Lei nº 12.527, de 18 de novembro de 2011](#)

III - nos casos em que os dados forem acessíveis publicamente, observadas as disposições desta Lei.

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou

V - na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos

dados, desde que vedado o tratamento para outras finalidades.

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.

Foi nesse ímpeto de tentar colmatar as lacunas da LGPD no tocante ao tratamento de dados pelo Poder Público que, no ano passado, foram editados dois importantes atos infralegais: o Decreto 9.929/2019, que criou o Sistema Nacional de Informações de Registro Civil – SIRC e o Decreto 10.046, de 9 de outubro de 2019, que instituiu o chamado Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. **Esse último decreto é apontado pela União como o ato normativo que ampara o ato do Poder Público impugnado nesta ADPF**.

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

O ato normativo ainda dispensa a autorização prévia do gestor dos dados para o compartilhamento, estabelecendo que este será realizado mediante “*canais existentes para dados abertos e para transparência ativa*” (art. 11). Além disso, a grande inovação do Decreto é a instituição do Cadastro Base do Cidadão, que corresponde a uma espécie de “cadastro geral nacional”. Esse cadastro é composto principalmente pelos dados biográficos que constam da base temática do CPF, contendo atributos específicos como nome completo, nome social, data de nascimento, sexo, filiação, nacionalidade, naturalidade e outros (art. 18). Essa espécie de

ADPF 695 MC / DF

“lago de dados” pode ser indistintamente utilizada no âmbito do Poder Público.

Nesse aspecto, percebe-se que as únicas salvaguardas ao processamento dos dados estabelecidas pelo Decreto têm a ver com a disciplina do sigilo dos dados dentro dos níveis e regras de segurança. Limitações adicionais a esse regime de compartilhamento só podem ser impostas pelo Comitê Central de Governança de Dados, órgão governamental responsável por definir as regras e os parâmetros para o compartilhamento restrito de dados, de acordo com os padrões relativos à preservação do sigilo e da segurança e por coordenar a integração das bases de dados na Administração Pública (art. 21). Ressalte-se que o Comitê é composto exclusivamente por membros do Governo, sem qualquer representação da sociedade civil (art. 22).

Da simples leitura do Decreto, não é necessário grande esforço para se chegar à conclusão, já alinhavada por estudiosos sobre o tema, de que o Decreto do Cadastro Único “*é uma verdadeira carta branca para a circulação irrestrita de dados, inclusive os de natureza pessoal, na Administração Pública, tudo em nome da eficiência e melhorias na prestação dos serviços públicos*” (MARANHÃO, Juliano e CAMPOS, Ricardo. **A divisão informacional de Poderes e o Cadastro Base do Cidadão**. Portal Jota. Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/artigos/a-divisao-informacional-de-poderes-e-o-cadastro-base-do-cidadao-18102019).

A despeito das críticas a esse Decreto, **não é possível afirmar in abstracto que todo e qualquer compartilhamento de dados pelo Poder Público nele baseado afigura-se inconstitucional**. É que, do ponto de vista da jurisdição constitucional, cabe analisar em cada caso concreto em que medida a restrição imposta ao direito fundamental à proteção de dados pessoais revela-se excessiva considerando-se as particularidades do compartilhamento em questão.

Dessa maneira, o que cumpre examinar em situações como a ora colocada é de que maneira o regime precário de salvaguardas

ADPF 695 MC / DF

estabelecido nesse ato normativo pode eventualmente expor a riscos o direito à autodeterminação informativa, tanto a partir da respectiva base legal autorizadora do tratamento quanto do exame da proporcionalidade desse tratamento *vis a vis* a finalidade indicada.

2.1.5 – Da ausência de base legal para o compartilhamento de dados entre DENATRAN e ABIN e do teste de proporcionalidade do ato do Poder Público

A partir dos pressupostos assentados no presente voto, é possível deduzir que o processamento de dados pessoais pelo Poder Público deve se basear em fundamentos legais claros e específicos e deve perseguir uma finalidade legítima e proporcionalmente compatível. Assim, cumpre examinar, no caso em tela, se o compartilhamento entre o DENATRAN e a ABIN ancora-se em alguma previsão legal válida.

A União defende que o compartilhamento dos dados de CNH de 76 milhões de brasileiros entre o DENATRAN e ABIN estaria inserido no âmbito da atividade de inteligência da ABIN, estabelecida no art. 5º da Lei 9.883/1999 e instituída pelo Decreto 8.793, de 29 de junho de 2016, consagrando entre seus objetivos a identificação de fatos ou situações que possam resultar em ameaças ou riscos à promoção da segurança e dos interesses do Estado e da sociedade brasileira.

Essa visão, a propósito, foi espelhada na manifestação da ABIN juntada aos autos, em que se afirma que “a consulta aos dados constantes dos sistemas do DENATRAN pela ABIN favorecerá a apuração de irregularidades ligadas, especialmente, à criminalidade organizada, à corrupção, ao terrorismo e às práticas ilegais envolvendo o comércio de bens de uso dual e de tecnologias sensíveis, quatro das principais ameaças à integridade do Estado e da sociedade e à segurança nacional identificadas na PNI”.

O principal argumento trazido pela União, portanto, seria o de que o compartilhamento de dados entre DENATRAN e ABIN estaria amparado na própria lei que estipula as diretrizes da Política Nacional de

Inteligência (PNI). **Essa tese, no entanto, não parece compatível com uma interpretação sistemática dessa legislação.**

O objetivo da lei que institui o Sistema Brasileiro de Inteligência (SISBIN) consiste em integrar ações de planejamento e execução das atividades de inteligência do país com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional. É claro que, no âmbito da execução de atividades de inteligência, o processamento de dados pessoais revela-se fundamental. Daí porque o art. 4º da lei buscou, na medida do possível, regulamentar o planejamento e a execução de atividades sigilosas na produção de conhecimentos destinados ao assessoramento da Presidência da República. Destaca-se o teor do dispositivo:

“Art. 4º À ABIN, além do que lhe prescreve o artigo anterior, compete:

I - planejar e executar ações, inclusive sigilosas, relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o Presidente da República;

(...) Parágrafo único. Os órgãos componentes do Sistema Brasileiro de Inteligência fornecerão à ABIN, nos termos e condições a serem aprovados mediante ato presidencial, para fins de integração, dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais”.

Verifica-se que o art. 4º, parágrafo único, da lei, ao contemplar a análise de dados como etapa essencial das atividades de inteligência, esclareceu a possibilidade de compartilhamento de dados entre os órgãos componentes do Sistema Brasileiro de Inteligência.

Todavia, **a legislação não dispõe sobre esse compartilhamento entre órgãos e entidades da Administração Pública que não integram referido Sistema Brasileiro de Inteligência.** Por isso, não há como intuir – como defende a União – que a mesma base legal que possibilita o compartilhamento *interna corporis* no Sistema Brasileiro de Inteligência

ADPF 695 MC / DF

necessariamente também serviria de amparo para a cooperação com órgãos de fora desse sistema.

Outra hipótese que se poderia cogitar é a de que as próprias disposições da LGPD e do Decreto 10.046/2020 legitimariam o compartilhamento. Essa tese, ainda que pudesse se fazer tangível ante a aplicabilidade explícita dessa lei e do referido decreto às relações com o Poder Público, suscita inúmeras dificuldades.

Em primeiro lugar, sabe-se que, malgrado o Decreto 10.046/2020 tenha referenciado a sistemática da LGPD, essa lei ainda não se encontra em vigor no ordenamento jurídico.

Além disso, observa-se que **o próprio texto da LGPD escusa a aplicação dos seus princípios e diretrizes ao tratamento de dados para fins de segurança pública, defesa nacional ou segurança do estado (art. 4º, inciso III).**

Ademais, mesmo que fosse possível cogitar da aplicabilidade da LGPD, como já analisado no presente voto, as bases legais específicas para o tratamento de dados pelo Poder Público nessa lei parecem estar totalmente vinculadas à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7, inciso III).

Nesse ponto, a União destaca na ementa de sua manifestação que as atividades de inteligência constituem um tipo de política pública e que, por isso, seria finalidade admitida como legítima para respaldar o compartilhamento de dados entre órgãos e entidades da Administração Pública.

Contudo, como já afirmado no presente voto, são bastante vagas as balizas de aplicação da LGPD às atividades de tratamento de dados pelo Poder Público. Além disso, a própria lei geral, malgrado tome a referência à execução de serviços públicos como cláusula geral para o tratamento, demanda que a finalidade do tratamento seja minimamente colmatada em legislação específica, o que, como visto, não parece ocorrer no âmbito do SISBIN.

Todos esses fatores indicam que, *a priori*, não há uma autorização

ADPF 695 MC / DF

irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no Poder Público, inclusive para realização das atividades de inteligência nacional. Desse modo, convênios e acordos de compartilhamento baseados única e exclusivamente nas disposições do Decreto 10.046/2020 parecem afigurar-se potencialmente lesivos às garantias individuais discutidas nesta ADPF, a depender, é claro, das condições de compartilhamento e dos riscos envolvidos.

De todo modo, ainda que se admitisse que o Termo de Autorização 7/2020 e o ato do Poder Público impugnado nesta ADPF apresentam bases legais sólidas, **isso não afastaria a necessidade de se examinar, sob a perspectiva constitucional, em que medida as restrições impostas por esse ato ao direito fundamental à proteção são proporcionais.**

Desde a concepção do direito à privacidade como manifestação do direito à autodeterminação informacional pela Corte Constitucional alemã, já se reconhece que o princípio da proporcionalidade desempenha relevante papel de aferição da constitucionalidade das interferências à proteção jurídica da autodeterminação informacional. O teste da proporcionalidade, a propósito, foi central na construção realizada pelo *BVerfG* a partir do julgamento da Lei do Censo de 1983.

O teste de proporcionalidade é plenamente aplicável às relações de tratamento de dados no setor público. A incidência do princípio da finalidade nessas relações não deve se limitar à busca por uma base legal – que no presente caso sequer é existente – mas deve levar em consideração também elementos como (i) as expectativas razoáveis do titular, (ii) a natureza dos dados processados e (iii) os possíveis prejuízos a serem suportados pelo titular. (ALSENOY, B. V.; KINDT, E.ç DUMORTIER, J. **Privacy and Data Protection Aspects of e-Government Identity**. In: *Innovation Government: Normative, Policy and Technological Dimensions of Moderns Government* Haia: Springer, 2011, p. 255).

Todos esses elementos são passíveis de internalização no teste da proporcionalidade. Como bem destacado em artigo escrito por **Gillian Black** e **Leslie Stevens**, a proporcionalidade tem sido o principal

parâmetro utilizado no Direito Europeu para a aferição da constitucionalidade do tratamento de dados no setor público. Os autores desenvolvem uma aplicação trifásica desse teste, o qual reflete as tradicionais fases de valoração da *adequação*, necessidade e proporcionalidade em sentido estrito. (BLACK, Gillian e STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest**. Scripted. Vol. 10, n. 1, 2013).

Do ponto de vista da *necessidade*, cumpre avaliar se o processamento ou compartilhamento dos dados pelos órgãos converge para um legítimo objetivo de política pública ou para o exercício de uma obrigação legal dos órgãos públicos envolvidos.

Do ponto de vista da *adequação*, cumpre avaliar quais os riscos envolvidos no processamento dos dados em questão e qual a possibilidade de dano aos indivíduos titulares. Também nessa fase, revela-se necessário entender se a medida adotada é a menos invasiva possível para o resultado visado.

Já na aferição da *proporcionalidade em sentido estrito*, o que deve ser examinado é se o interesse público atinente a esse processamento é superior ao interesse público da coletividade envolvido na vulneração da proteção dos dados pessoais.

A fim de orientar a aplicação dessas fases, Gillian Black e Leslie Stevens orientam a formulação dos seguintes quesitos que devem ser respondidos pelo controlador para se verificar se o método de tratamento é proporcional para consecução dos objetivos (BLACK, Gillian e STEVENS, Leslie. **Enhancing Data Protection And Data Processing In The Public Sector: The Critical Role Of Proportionality And The Public Interest**. Scripted. Vol. 10, n. 1, 2013, p. 97). Destacam-se as questões apontadas pelos autores:

- “i. O tratamento proposto dos dados pessoais é o meio menos intrusivo para atingir o objetivo do órgão público?
- ii. O processamento está de acordo com os demais princípios de proteção de dados incluindo, criticamente, o

ADPF 695 MC / DF

terceiro princípio de proteção de dados, o qual requer que os dados pessoais processados não devem ser excessivos?;

iii. A anonimização pode ser utilizada e, em caso afirmativo, é a técnica proposta considerado efetivo?

iv. A proposta de processamento foi aprovada por um órgão competente?

v. Foi realizada uma avaliação de impacto na privacidade para avaliar e mitigar os riscos inerentes ao processamento em questão?

vi. Existe um interesse público identificável no processamento dos dados pessoais?

vii. Existe um interesse público identificável em fornecer ao público relevante serviços?"

No caso em tela, há uma enorme dificuldade em proceder ao teste de proporcionalidade em todas as suas etapas. Isso porque, 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 nem sobre a natureza dos dados compartilhados tampouco acerca dos parâmetros objeto do compartilhamento.



Ressalte-se que, por disposição expressa do art. 5º do Decreto 10.0406/2019, “fica dispensada a celebração de convênio, acordo de cooperação técnica ou instrumentos congêneres para a efetivação do compartilhamento de

ADPF 695 MC / DF

dados entre os órgãos". Assim, dificilmente os órgãos envolvidos no compartilhamento tornariam público no futuro os termos em que o compartilhamento visado ocorreria. A fim de se afastar qualquer dúvida quanto ao caráter obscuro do termo de autorização, colacione-se abaixo o extrato publicado no DOU:



Fonte: e-DOC 15

Assim, do ponto de vista da adequação, seria bastante difícil examinar o ato em questão, já que a única face pública da medida, como dito, adota redação essencialmente genérica ao indicar os objetivos do compartilhamento de dados e sequer explicita a finalidade para as atividades de inteligência.

Já sob o prisma da necessidade, também 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 onde recaia 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 cotejar 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 obscura de tratamento de dados para atividades de vigilância não conhecidas.

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

ADPF 695 MC / DF

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.

3 – Do perigo na demora

Além da verossimilhança das alegações, em uma análise inicial, também entendia que restaria atendido no caso concreto o requisito do *periculum in mora*. É que, como consta da própria manifestação da União juntada aos autos (eDOC 14) a ABIN de fato enviou ao DENATRAN o Ofício 269/2019/SPG/ABIN/GSI/PR de 29.11.2019, por meio do qual solicitou acesso às bases de dados daquele órgão, com o objetivo de incrementar o exercício de suas atribuições. Além disso, após esse pedido, o DENATRAN concedeu à ABIN o Termo de Autorização 7/2020 e orientou o órgão receptor a entrar em contato com o SERPRO para a celebração de contrato administrativo.

Ocorre que, **na véspera da apreciação do pedido de medida cautelar nesta ADPF pelo Plenário do STF**, a União peticionou nos autos (eDOC 28) informando que o Termo de Autorização 7/2020 foi revogado na data de 23.06.2020. Confira-se o teor da manifestação do ente público:

Conforme consignado em petição de 22/06/2020, a ABIN de fato solicitou acesso à base de dados do DENATRAN, mediante pedido processado conforme à Portaria nº 15/2016/DENATRAN. A requisição que foi deferida na forma do Termo de Autorização nº 7/2020, do DENATRAN, publicado no Diário Oficial da União – DOU Nº 46, Seção 3, de 9 de março de 2020.

Esse ato concreto – o termo de autorização – é que efetivamente deveria ter sido impugnado pelo arguente, pois é ele que estabelece a chancela, as condições e os limites do compartilhamento impugnado na inicial, tal como salientado em tópico preliminar da manifestação anterior do Advogado-

ADPF 695 MC / DF

Geral da União. Cumpre enfatizar que o compartilhamento não chegou sequer a ser operacionalizado, uma vez que o imprescindível contrato com o SERPRO, necessário à disponibilização das informações (artigo 22 da Portaria nº 15/2016/DENATRAN) ainda não fora celebrado.

Embora a autorização nem tenha chegado a surtir efeitos práticos, a Secretaria Nacional de Transportes Terrestres, do Ministério da Infraestrutura, diligenciou ativamente pela sua revogação, conforme consta da Nota Técnica nº 626/2020/CGATF-DENATRAN/SNTT (anexa), da qual se convém transcrever o seguinte excerto:

3.6. Não obstante, considerando os argumentos ofertados no processo judicial em comento, à luz do Princípio da Autotutela, entende-se oportuno que o Termo de Autorização nº 7/2020-A (SEI nº 2398687), emitido por este Departamento em favor da ABIN, com amparo na Portaria DENATRAN nº 15, de 18 de janeiro de 2016, publicado no Diário Oficial da União - DOU N° 46, Seção 3, de 9 de março de 2020, seja revogado e, em seguida, reavaliados os critérios que levaram à publicação do referido Termo de Autorização.

3.7. Vale destacar que, até o momento, não foi celebrado o necessário contrato administrativo com o SERPRO para possibilitar à ABIN o acesso autorizado pelo DENATRAN. Conforme preveem os arts. 5º e 22 da Portaria DENATRAN nº 15, de 18 de janeiro de 2016, que estabelece os procedimentos para acesso aos dados dos sistemas e subsistemas informatizados do DENATRAN, a disponibilização das informações só se opera mediante a celebração de contrato com o SERPRO, após a autorização deste Departamento, senão vejamos:

Art. 5º Será admitida a disponibilização continuada e periódica de informações, mediante celebração de contrato com

ADPF 695 MC / DF

o Serviço Federal de Processamento de Dados –SERPRO, após prévia autorização do DENATRAN. (g.n.)

Art. 22. Após autorizado o acesso pelo DENATRAN, o interessado deverá celebrar contrato como SERPRO, empresa pública federal responsável pela operação dos sistemas e subsistemas do DENATRAN. [...] (g.n)

3.8. Salienta-se que, com a revogação do ato administrativo ora proposta, não haverá qualquer outra providência a ser adotada pelo DENATRAN em relação ao presente caso, pois o acesso aos sistemas DENATRAN, por parte da ABIN, não se efetivou em razão de que, repita-se, ainda não houve a prévia celebração de contrato com o SERPRO.

Também anexo segue o documento de revogação do Termo de Autorização, devidamente assinado pelo Diretor-Geral do DENATRAN, encaminhado para publicação na Imprensa Oficial.

A iniciativa de revogação insere-se em um plano de ação mais amplo no âmbito do DENATRAN, voltado a revisar os termos da política de compartilhamento destes dados, de modo a fazê-la condizente com parâmetros jurídicos recentemente estabelecidos, como os fixados por esse próprio Supremo Tribunal Federal no âmbito da Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6387, cujo acórdão ainda aguarda publicação.

Observa-se, portanto, a União voluntariamente revogou o Termo de Autorização no exercício de autotutela da Administração Pública e afirma que, por se tratar de ato preparatório, não teria havido a efetivação do compartilhamento de dados entre as entidades, uma vez que ainda restava pendente a celebração de contrato com a SEPRO.

Dessa maneira, entendo que não mais persiste o perigo na demora que embasaria a concessão da medida cautelar pleiteada especificamente

ADPF 695 MC / DF

para afastar definitivamente o compartilhamento de dados entre o DENATRAN e a ABIN.

4 – Da ausência de perda de objeto da ADPF

Sem embargos da revogação do Termo de Autorização 7/2020, verifico que o ato do poder público impugnado nesta ADPF é mais amplo e abrange, como um todo, o plexo de medidas tendentes ao compartilhamento de dados pessoais pelos órgãos e entidades da Administração Pública com suposto lastro normativo no Decreto nº. 10.046, de 9 de outubro de 2019 (eDOC 1, p. 2).

Nesse sentido, como já aduzido na presente decisão, além do pedido de suspensão de compartilhamento dos dados da base da CNH com a ABIN, o requerente formulou pleito subsidiário para que seja dada interpretação conforme à Constituição ao Decreto nº. 10.046, de 9 de outubro de 2019, a fim de que: “(i) o rol de finalidades exposto no art. 1º deste ato normativo, seja considerado taxativo e exaustivo, de modo que o tratamento se dê apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, à luz do princípio da finalidade que norteia a proteção de dados pessoais constitucionalmente garantida no país; (b) diante da interpretação acima, expressamente se afaste da abrangência do referido Decreto a finalidade de atividade de inteligência, visto que não prevista no ato normativo em causa; e, (c) à luz do previsto nos incisos I, V e VI do art. 3 do referido Decreto, se garanta expressamente que o compartilhamento de dados pessoais por órgãos e entidades do setor público está expressamente sujeito e vinculado aos princípios que balizam a proteção de dados pessoais no Brasil, expressos no art. 6º da Lei nº 13.709, de 2018, especialmente quanto à finalidade, adequação, necessidade e transparência” (eDOC 1, p. 32).

Dessa maneira, ainda que tenha quedado ausente o requisito de perigo na demora especificamente quanto ao pedido de suspensão do compartilhamento de dados da base do DENATRAN materializado no

ADPF 695 MC / DF

Termo de Autorização 7/2020, resta pendente de análise, por este STF, a alegação de que as disposições do Decreto nº. 10.046, de 9 de outubro de 2019 violam *in abstracto* o disposto no art. 5º, caput e incisos X e XII, da Constituição Federal.

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

Por esse motivo, é dever constitucional deste STF debruçar-se sobre a matéria, evitando-se que situações graves que colocam em risco a violação de preceitos fundamentais sejam perpetradas com suposto fundamento no Decreto nº. 10.046, de 9 de outubro de 2019. Destaca-se ainda que a presente decisão não obsta a eventual análise de medida acauteladora relacionada à alegações de inconstitucionalidade deste ato normativo.

5 – Dispositivo

Ante o exposto, ausentes os pressupostos para a concessão da tutela de urgência, indefiro, *ad referendum* do Plenário do Supremo Tribunal Federal, o pedido de medida cautelar (art. 21, V, do RISTF).

Intimem-se o requerente, o Advogado-Geral da União e o Procurador-Geral da República, para que, no prazo de dez dias, manifestem-se sobre o objeto da presente ADPF, se entenderem necessário, nos termos do art. 6º, *caput* e § 1º, da Lei 9.882/1999.

Publique-se.

Brasília, 24 de junho de 2020.

Ministro **Gilmar Mendes**
Relator

ADPF 695 MC / DF

Documento assinado digitalmente