# Sustentação oral na ADI n. 6649

Danilo DONEDA[*]

31.08.2022[**]

Excelentíssimo Sr. Presidente desta Corte Suprema;
Excelentíssimo Sr. Ministro Relator;
Excelentíssimos Sras. e Srs. demais integrantes desta Corte;
Eminente Sr. Vice Procurador-Geral da República;
Caras e caros Colegas;
Senhoras e Senhores,

O que está em jogo hoje é assegurarmos que a modernização da administração pública, através de uma gestão e planejamento que façam uso de informações, seja acompanhada de garantias contra os riscos ao cidadão derivados do tratamento de seus dados pessoais; o que está em jogo é garantir que os custos desta modernização não recaiam sobre o cidadão, que tem o direito de poder continuar confiando no Estado como depositário de seus dados pessoais. O que está em jogo hoje nada mais é, enfim, do que adequar a ordem jurídica aos dilemas e demandas de nosso tempo.

Venho, em nome do CONSELHO FEDERAL DA ORDEM DOS ADVOGADOS DO BRASIL, apresentar as razões pelas quais requeremos a declaração de inconstitucionalidade do Decreto n. 10.046, de 2019.

O Decreto dispõe sobre compartilhamento de dados no âmbito da administração pública federal. Ele, porém, desarma um conjunto de garantias que são necessárias para o

[*] Advogado. Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professor no Instituto Brasiliense de Direito Público (IDP). Foi membro indicado pela Câmara dos Deputados para o Conselho Nacional de Proteção de Dados e Privacidade. Bacharel em Direito pela Universidade Federal do Paraná (UFPR). Foi Coordenador-Geral na Secretaria Nacional do Consumidor do Ministério da Justiça; membro da Comissão de Juristas formada pela Câmara dos Deputados para redigir projeto de lei sobre proteção de dados nos setores de segurança pública e investigação criminal; membro do Grupo de Trabalho sobre proteção de dados e informações judiciais do Conselho Nacional de Justiça; membro dos conselhos consultivos do Projeto Global Pulse (ONU), do Projeto Criança e Consumo (Instituto Alana) e da Open Knowledge Brasil. Consultor do Comitê Gestor da Internet no Brasil (CGI.br); membro do conselho editorial da Revista de Derecho Digital (Espanha); e pesquisador visitante na Autoridade Garante para a Proteção de Dados em Roma (Roma, Itália), na Università degli Studi di Camerino (Camerino, Itália) e no Instituto Max Planck para Direito Privado Comparado e Internacional (Hamburgo, Alemanha).

[**] A publicação póstuma da presente sustentação, gentilmente autorizada pelos familiares do autor, faz parte das homenagens prestadas pela Civilistica.com ao inestimável legado deixado pelo Prof. Danilo Doneda ao direito civil brasileiro. Que os frutos da sua atuação pioneira na tutela da privacidade e dos dados pessoais continuem fazendo a diferença nos anos vindouros.

exercício da cidadania em uma sociedade ávida pela informação, garantias estas que foram duramente conquistadas e consolidadas pelo direito fundamental à proteção de dados e pela LGPD – Lei Geral de Proteção de Dados. Assim, este compartilhamento, que é imprescindível para a eficácia dos mais modernos métodos de gestão, acaba por se converter em fator de insegurança e ilegalidade, além de alijar o cidadão do controle e ciência sobre a utilização de seus dados pelo Poder Público.

Esta inconstitucionalidade se faz evidente por motivos formais e materiais. Formalmente, manifesta-se com clareza a extrapolação da competência regulamentar pelo Presidente da República: Ao procurar regulamentar as leis 12.527/2011 (LAI), 13.444/2017 (ICN) e 13.709/2018 (LGPD), opera o Decreto concreta inovação no ordenamento jurídico ao dispor sobre direitos e garantias fundamentais dos cidadãos, limitando-as concretamente, bem como aumentando os riscos a que os cidadãos estão expostos.

Este Decreto foi sancionado nos estertores de um paradigma hoje vetusto e ultrapassado. Seu texto remonta a uma época na qual dificuldades crônicas de acesso a informações para alimentar políticas públicas eram tais que dados pessoais eram muitas vezes usados de forma virtualmente irrestrita e sem garantias para os cidadãos. Este cenário, no entanto, mudou rápida e radicalmente com o desenvolvimento de tecnologias de processamento de dados, gerando a necessidade da regulação destes tratamentos justamente para contemplar a proteção do cidadão – enfim, é justamente para adequar o sistema de garantias constitucionais às novas tecnologias dominantes que surgiu uma legislação como a LGPD. Neste novo paradigma, os dados pessoais deixaram de ser um recurso escasso e juridicamente pouco relevante para ter, inclusive, um valor jurídico intrínseco – como se tornou costume mencionar, os dados pessoais se tornaram o combustível da nova economia da informação – assim como sua proteção se tornou essencial para a garantia da cidadania.

O Decreto, no entanto, como se a modernidade lhe fosse estranha ou inconveniente, parece ignorar este novo paradigma ao considerar a informação pessoal sob prisma meramente utilitarista e tecnocrático, em frontal desacordo com o que afirmou esta Excelsa Corte em julgamento paradigmático de 2020 quando da propositura por este CF-OAB e por uma série de partidos políticos de ADIs em face da MP n. 954, que pretendia justamente o compartilhamento de dados pessoais entre dois entes públicos sem maiores salvaguardas para os cidadãos. Naquela ocasião, constatou esta Corte que não existem mais dados pessoais insignificantes: isto é, todo tratamento de dados pessoais apresenta

um potencial de risco intrínseco que demanda a implementação de mecanismos de proteção aos titulares para que possa se legitimar em uma sociedade democrática.

Com aquela decisão, a proteção de dados no Brasil passou a proporcionar a garantia dos direitos inalienáveis do cidadão na era digital, posicionando-se na nossa ordem jurídica como instrumento para a consolidação da democracia e das liberdades. Hoje, a partir de seus dados pessoais, cidadãos podem ser analisados, avaliados, monitorados, discriminados e... controlados, além de extirpados de sua autonomia e dignidade por frequentes decisões que afetam suas vidas serem tomadas a partir de seus dados, sem o devido processo e sem que tenham oportunidade de participação. É assim, aliás, que assevera a Profª. Laura Schertel Mendes em artigo publicado recentemente no jornal *O Globo*, no qual destaca como o poder informacional, que é derivado do controle sobre o uso da informação, pode ser malversado a prejuízo dos direitos e garantias fundamentais.

Materialmente, verificamos que o Decreto não estabelece o devido equilíbrio entre o compartilhamento de dados pessoais com os imperativos decorrentes do direito fundamental à proteção de dados, pelos motivos elencados em nosso pedido e que passo a resumir muito sucintamente.

Em primeiro lugar, o referido Decreto é silente quanto aos riscos potenciais aos cidadãos resultantes do compartilhamento. Esta lacuna é ressaltada pelo fato da categoria de dados sensíveis – aqueles que apresentam maior potencial discriminatório –, ser solenemente ignorada pelo Decreto que, por outro lado, não se furta a validar tratamentos de dados que são, de fato, sensíveis - por exemplo, dados biométricos, como quando se refere a "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (art. 2º, II, do Decreto nº 10.046/2019).

O Decreto não esboça qualquer regime particular de proteção para estes dados.

O decreto prossegue seu rol de desacertos ao menoscabar o princípio da transparência e, ainda, em diversos momentos aumentar uma opacidade que já é intrínseca aos tratamentos de dados, como quando possibilita a interligação de bases de dados de diferentes órgãos públicos sem a necessidade de acordos ou convênios entre estes.

Outra lacuna clamorosa do Decreto, no que talvez seja a sua falha estrutural que mais o caracteriza como uma normativa ultrapassada, é a ausência de mecanismos que proporcionem o devido controle e transparência acerca da finalidade para a qual os dados pessoais são compartilhados pela Administração Pública. A LGPD prevê uma base legal para o tratamento de dados pela Administração Pública que, no entanto, restringe-se aos dados que são necessários para as suas atividades específicas, nunca para uma cadeia genérica, indefinida e indeterminada de finalidades que podem ser inadequadas ou não relacionadas.

O tratamento de dados pelo setor público não é uma finalidade em si, ainda que o Decreto pareça pressupor que o seja. A finalidade que justifica este tratamento deve ser considerada e avaliada de acordo com as competências dos órgãos envolvidos, as políticas públicas em questão, a natureza dos dados e uma série de outros elementos. A hipertrofia da finalidade do tratamento que é operada pelo Decreto implica, na prática, na formulação de uma verdadeira nova base legal, extrapolando em muito, portanto, o poder regulamentar.

Seria natural que, do Decreto, constassem soluções úteis e inovadoras para a garantia do direito fundamental à proteção de dados - porém não é isso que ocorre, criando-se o grave risco de consolidação de práticas que fulminam os direitos fundamentais e erodem a confiança do cidadão nos agentes públicos. Ante estes riscos, um sistema de otimização da gestão de políticas públicas, como o Cadastro Base do Cidadão, por exemplo, pode facilmente se transmudar em ferramenta de vigilância e controle social, ainda mais se eventualmente cair em mãos de um governo com pouco apreço pelas liberdades democráticas – por isto, justamente, as garantias sobre dados pessoais não dizem respeito somente a interesses individuais, porém detêm função da maior importância para o Estado Democrático de Direito.

Felizmente, há diversas formas de sanar as deficiências do Decreto. Várias medidas capazes de garantir a legitimidade do compartilhamento de dados devem ser consideradas, tais como (1) a efetiva verificação de compatibilidade de finalidades nos compartilhamentos; (2) a consideração do risco inerente, com a instituição de medidas de avaliação de risco e atenção particular aos dados sensíveis; (3) a criação de plataformas que promovam a transparência em relação ao uso dos dados pessoais e que permitam ao cidadão exercer seus direitos e realizar escolhas relevantes sobre a utilização de seus dados, dentre outras - todas estas ausentes do Decreto.

Ademais, no contexto do julgamento no qual esta Egrégia Corte havia reconhecido, em 2020, o direito fundamental à proteção de dados, foram identificados diversos parâmetros para a sua implementação, consolidando um verdadeiro arcabouço para balizar o compartilhamento de dados pessoais. Estes elementos englobam, além dos que já mencionamos, a necessidade da (1) construção de um sistema de governança dos dados pessoais acessível ao cidadão e capaz de proporcionar as necessárias garantias, (2) a avaliação da real necessidade e pertinência do uso de dados pessoais e, muito importante, (3) a proporcionalidade deste uso em relação aos fins almejados; (4) a consideração da efetividade dos direitos dos titulares de dados; (5) a elaboração de mecanismos de segurança proporcionais aos riscos presentes, dentre vários outros. A ausência deste conjunto de garantias, hoje, ameaça calcificar práticas deletérias às liberdades fundamentais, empacotadas dentro de burocráticas rotinas administrativas que são impermeáveis aos reais efeitos dos tratamentos dos dados pessoais aos cidadãos e à sociedade.

A proteção de dados no Brasil é uma disciplina para cuja legitimidade e formação contribuíram diversos atores, desde a propositura do Anteprojeto de Lei sobre Proteção de Dados pelo Poder Executivo, passando pelo protagonismo do Poder Legislativo ao encaminhar a matéria até culminar com o reconhecimento por esta Egrégia Corte do Direito Fundamental à Proteção de Dados - a partir do que o caminho trilhado não teria mais retorno.

Paradigmas, no entanto, costumam ser ultrapassados gradualmente. Cabe, neste momento, ao se decidir sobre a constitucionalidade do Decreto n. 10.046, proporcionar ao cidadão segurança para que reconheça no Estado um digno depositário de seus dados, em uma relação que, ao cabo, é indispensável para que se possibilite o uso e compartilhamento de dados com legitimidade, segurança e sob os auspícios da boa-fé e no marco da defesa do Estado Democrático de Direito.

A atual estrutura do Decreto 10.046 torna inviável esta superação de paradigma. Sua manutenção consolidaria um sistema dúplice de proteção de dados, um para os tratamentos realizados pelo setor privado e outro, débil e desarticulado, para o setor público, configurando óbice à consolidação do direito fundamental à proteção de dados na ordem jurídica pátria, com o agravante de incidir com maior gravidade em relação aos direitos da parcela da população de menor poder aquisitivo ou em situação de vulnerabilidade, para os quais os serviços públicos são ainda mais importantes ou imprescindíveis. Eventualmente, pode ser pertinente que a cessação dos efeitos do

Decreto seja modulada em termos definidos por esta Egrégia Corte, de forma a não interromper tratamentos de dados de maior relevância e menor potencial de risco, até o momento em que vier a advir legislação que contemple o novo paradigma, que se afigura, conforme verificamos, ser indispensável e da máxima urgência.

Por todo o exposto, o Conselho Federal da Ordem dos Advogados do Brasil, em iniciativa que contou com a valorosa e indispensável liderança e empenho, entre tantos, das advogadas e advogados Estela Aranha, Lúcia Teixeira Ferreira, Ilton Robl Filho e Marcus Vinícius Furtado Coelho requer, reconhecida a natureza constitucional do direito à proteção de dados pessoais e as razões de fato e de direito aqui aludidas, a declaração da inconstitucionalidade do Decreto 10.046, de 9 de outubro de 2019 em sua íntegra.

**Como citar:**

DONEDA, Danilo. Sustentação oral na ADI n. 6649. **Civilistica.com**. Rio de Janeiro, a. 11, n. 3, 2022. Disponível em: <http://civilistica.com/sustentacao-oral-na-adi-6649/>. Data de acesso.