

Ferreira: A inconstitucionalidade do Decreto 10.046/2019 e o STF

24/02/2022

Nesta quinta-feira (24/2), o Plenário do Supremo Tribunal Federal iniciará o julgamento da Ação Direta de Inconstitucionalidade (ADI) nº 6.649/DF, relatada pelo ministro Gilmar Mendes e proposta pelo Conselho Federal da OAB em dezembro de 2020. A mencionada ADI postula a declaração de inconstitucionalidade do Decreto 10.046/2019, que *"dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados"*, tendo em vista que o referido ato infralegal exorbita os poderes normativos concedidos ao presidente da República pela Constituição Federal e viola os direitos fundamentais à dignidade da pessoa humana, à intimidade, à privacidade, ao sigilo dos dados e à proteção de dados pessoais.



Sob o argumento de que as medidas previstas no

Decreto nº 10.046/2019 facilitarão o acesso dos brasileiros a serviços públicos federais, o referido decreto estabelece regimes e práticas para o tratamento de dados pessoais pela Administração Pública federal, à revelia do direito fundamental à proteção de dados pessoais e de diversas disposições presentes na Lei Geral de Proteção de Dados Pessoais, a LGPD (Lei 13.709/2018).

O direito à proteção de dados pessoais foi inserido expressamente no rol dos direitos fundamentais do artigo 5º da Constituição Federal pela Emenda Constitucional 115/2022, através do inciso LXXIX, nos seguintes termos: *"É assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais"*.

Entretanto, em uma histórica decisão datada de *maio de 2020*, o Plenário do STF *já havia reconhecido o direito à proteção de dados pessoais como um direito fundamental autônomo na ADI 6.387/DF*, quando o Plenário da corte referendou a medida cautelar deferida para suspender a eficácia da Medida Provisória 954/2020, que cuidava do compartilhamento de dados de milhões de usuários brasileiros de telefonia fixa e móvel com o Instituto Brasileiro de Geografia e Estatística (IBGE).

A partir desse julgado, consolidou-se um novo paradigma, reconhecendo-se o direito à proteção de dados pessoais como um *novo direito fundamental, destacado e independente do direito à privacidade*, o qual se configurava, na sua concepção tradicional, como uma garantia de abstenção do Estado na esfera privada individual.

No julgamento da medida cautelar da ADI 6.387/DF, o STF afirmou que a autonomia do direito fundamental à proteção de dados deriva do direito fundamental à dignidade da pessoa humana e da proteção constitucional à intimidade, à honra, à imagem e ao sigilo dos dados, principalmente diante do aumento de novos riscos aos direitos humanos resultantes do avanço tecnológico. Esse novo direito fundamental deriva, ainda, do reconhecimento do habeas data enquanto instrumento de tutela material do direito à autodeterminação informativa [1].

Tanto a decisão do STF de maio de 2020 quanto a efetiva introdução da proteção de dados pessoais no artigo 5º (inciso LXXIX) da Constituição Federal pela Emenda Constitucional 115/2022 devem ser celebradas como um extraordinário passo para o fortalecimento dos direitos fundamentais e como uma grande conquista da cidadania na era informacional.

Entretanto, em que pese a regulação infraconstitucional da proteção de dados pessoais efetivada através da LGPD, ainda existem contornos deste direito fundamental que precisam ser mais bem sedimentados. Alguns desses debates serão travados durante o julgamento da ADI 6.649, cujo resultado será essencial para a definição de critérios constitucionais relativos à atuação do Estado na coleta e no tratamento de dados dos cidadãos e no tocante aos parâmetros para compartilhamento de dados pessoais entre órgãos públicos e entre os entes estatais e os agentes privados.

É necessário destacar que o Decreto 10.046/2019 foi erigido com embasamento no paradigma anterior à referida decisão histórica do STF e à Emenda Constitucional 115/2022. Nesse paradigma anterior, conferia-se tutela constitucional apenas à privacidade e ao sigilo "da comunicação de dados", ou seja, não se reconhecia a tutela constitucional dos "dados em si mesmos" [2].

A gravidade e os riscos concretos para o cidadão estão presentes por todo o Decreto 10.046/2019 e este é desprovido de precauções organizacionais e processuais que previnam a violação de direitos dos cidadãos. Mencione-se, à guisa de exemplo, que o decreto, paralelamente a dados de diversas naturezas, menciona expressamente o tratamento de dados pessoais sensíveis sem as devidas salvaguardas, como dados biométricos, chegando a referir-se explicitamente 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*" (artigo 2º, II, do Decreto nº 10.046/2019) — sem que qualquer regime específico de proteção ou mesmo de justificativa para tal tratamento.

As chamadas base integradora e base temática previstas no artigo 2º, incisos VI e VII, do Decreto 10.046/2019 são *bases de dados que integrarão os atributos biográficos previstos no artigo 2º, I, e os atributos biométricos previstos no artigo 2º, II* e que provocam indagações sobre o contexto em que ocorrerão o tratamento e a utilização dessas novas bases e o

cruzamento desses dados. Insta frisar que tais informações, com o uso de técnicas de biometria comportamental e tecnologias de monitoramento, podem ser utilizadas para um controle político intenso dos cidadãos, típico de regimes totalitários.

O Decreto 10.046 contém regras relativas ao compartilhamento de dados pelos órgãos governamentais *em descompasso com a LGPD* e que permitem interligar bases e cruzar dados pessoais *sem critérios que sejam conhecidos dos cidadãos*, sem informações claras, adequadas e transparentes sobre a realização da coleta e do tratamento.

Além disso, não são evidenciados outros pontos essenciais do regime de proteção de dados pessoais instituído pelo respectivo direito fundamental e consolidado pela LGPD, como a identificação de quem são os agentes que fazem o tratamento, bem como qual é a compatibilidade com a finalidade para a qual a informação pessoal foi originariamente coletada.

Em função da normativa do Decreto 10.046/2019, os cidadãos brasileiros aceitam a coleta estatal de um dado pessoal para uma estipulada finalidade (como a execução de uma determinada política pública), com base no artigo 7º, inciso III, da LGPD. Contudo, passam a viver em um regime de permanente insegurança, posto que os dados coletados mediante aquela finalidade passam a ser utilizados seguidamente para uma outra finalidade e assim sucessivamente, sem o seu conhecimento.

Neste sentido, a LGPD prevê que o tratamento e compartilhamento de dados pela Administração Pública, entre as hipóteses elencadas nas bases legais do artigo 7º, restringe-se aos dados necessários para a execução daquela determinada política pública, não para uma cadeia indefinida e indeterminada de finalidades inadequadas e/ou obscuras.

A impossibilidade de se verificar a real finalidade do compartilhamento de dados é um aspecto que vulnera ainda mais o titular de dados pessoais. Nesse sentido, a própria amplitude dos órgãos envolvidos e sua heterogeneidade (conforme o artigo 1º do Decreto 10.046/2019, "entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União") representam uma situação de intenso risco para os titulares dos dados.

Ademais, *existem riscos de compartilhamento de dados através de convênios de acesso com empresas privadas, o que já vem ocorrendo e causando grande temor aos cidadãos*, haja vista que foi noticiada a formalização de convênios de acesso com empresas privadas, que, ao que tudo indica, se conectariam aos dados pessoais dos cidadãos brasileiros através do cadastro centralizado.

De forma temerária e violando normas da LGPD, *o Decreto 10.046/2019 é silente quanto à elaboração de relatórios de impacto de proteção de dados e sequer evidencia os mecanismos adequados de segurança da informação.* Os inúmeros incidentes de segurança ocorridos nas bases de dados do cadastro centralizado geridas pelo governo federal demonstram o descalabro da situação no tocante à ausência de mecanismos adequados de segurança da informação.

As justificativas trazidas pelos argumentos do governo federal no sentido de que o Decreto 10.046/2019 atribui "*maior eficiência na prestação de serviços públicos*" e "*implementa diretriz de viés desburocratizante*" apenas mascaram os perigos de que, em função dos propalados

benefícios do *governo digital*, estejam sendo implantados *mecanismos que se sobrepõem a direitos e garantias fundamentais*.

Um caso paradigmático sobre os riscos do governo digital para os direitos fundamentais ocorreu em 2020, quando o Tribunal Distrital de Haia, na Holanda, julgou uma ação contra o Estado holandês. Nesse julgado, o tribunal holandês determinou a interrupção imediata do SyRI — o sistema do governo holandês de indicação de risco — sob a alegação de que esse sistema representa um risco ao Estado democrático de Direito, além de violar direitos fundamentais.

O SyRI criava perfis de risco baseados em modelos de risco algorítmico sem o conhecimento dos cidadãos, com o intuito de identificar aqueles com maior probabilidade de cometer fraudes no sistema de benefícios sociais. O Tribunal Distrital de Haia concluiu que o uso do SyRI não encontrou um equilíbrio entre o direito à privacidade e o interesse público em detectar fraudes, indo contra o estabelecido no [artigo 8º da Convenção Europeia de Direitos Humanos \(CEDH\)](#), que prevê o direito à vida privada [3].

Em conclusão, esperamos que o STF declare a inconstitucionalidade do Decreto 10.046/2019 e que a sabedoria da corte possa conduzir o caso com a criação de regras e a utilização da modulação de efeitos para preservar direitos e assegurar o menor dano possível à previsibilidade e à segurança jurídica, promovendo, dessa forma, uma transição segura para a substituição do Decreto 10.046/2019 por outra norma infralegal que esteja consonante com os parâmetros constitucionais da privacidade e da proteção de dados pessoais e com as regras da LGPD.

[1] FERREIRA, Lucia Maria Teixeira. A decisão histórica do STF sobre o direito fundamental à proteção de dados pessoais. *Conjur*, 25 de set. de 2020. Disponível em: <<https://www.conjur.com.br/2020-nov-25/lucia-ferreira-stf-direito-protecao-dados-pessoais>>.

[2] Nesse sentido, o antigo paradigma da Corte Constitucional era na direção de que a tutela constitucional se destinava apenas à comunicação dos dados (ao sigilo das comunicações) e não aos dados propriamente ditos. Para mais detalhes: Supremo Tribunal Federal. RE 418.41/SC Julg. 10 maio 2006, DJe. 19.12.2006; Acórdão HC 91.867/PA, relator ministro Gilmar Mendes, Julg. 24.04.2012, DJe: 20.09.2012.

[3] Fonte: <https://internetlab.org.br/pt/itens-semanario/holanda-tribunal-decide-que-sistema-de-indicacao-de-risco-viola-direitos-humanos/>.

Fonte: <https://conjur.jumps.com.br/2022-fev-24/ferreira-inconstitucionalidade-decreto-100462019-stf/>