# Separação informacional de poderes e devido processo informacional

A assim chamada separação informacional de poderes, juntamente com o devido processo informacional, tem assumido cada vez mais atualidade e relevância, de modo especial no contexto da era


nas também para o Direito e para o Estado democrático de Direito.

O devido processo informacional constitui, de certo modo, uma decorrência lógica e exigência do Estado democrático de Direito contemporâneo, em razão da radicalidade das assimetrias, da sutileza e da pervasividade das novas tecnologias, e, consequentemente, das possibilidades de práticas abusivas que afetam ou potencialmente podem afetar o processo de tomada de decisão das pessoas em geral, especial, contudo, dos atores estatais encarregados da proteção e promoção dos direitos e garantias fundamentais). Por isso, o devido processo informacional implica a existência de instrumentos adequados ao estabelecimento de limites aos fatores referidos, como é o caso, e. g., da garantia da ampla defesa e do contraditório, assegurando condições de efetividade reais para o livre desenvolvimento da personalidade, dentre outros direitos e garantias fundamentais [1].

É nesse sentido, que — para ilustrar a questão — se revela imperiosa a vedação de bases de dados comuns, cujo compartilhamento é ilimitado entre e para todos os entes estatais. Dito de outro modo, é crucial que se assegure também uma separação/divisão informacional de poderes.

O devido processo informacional e a separação informacional de poderes devem ser compreendidos e concretizados numa perspectiva afinada com o assim designado constitucionalismo digital [2] , implicando, dentre outros aspectos, uma reconfiguração do Estado e do federalismo brasileiro, e, em virtude disso, do papel dos agentes estatais em razão da atualização do rol de direitos fundamentais, sobretudo a partir da promulgação da EC 115, que incluiu o direito à proteção de dados pessoais no catálogo constitucional.

Outrossim, urge, nesse mesmo contexto, levar a sério o dever constitucionalmente vinculativo, no sentido do desenvolvimento de uma gestão republicana, ética, confiável e segura dos dados durante todo o seu ciclo de vida, forjando as condições para o exercício da cidadania digital e, assim, o fortalecimento das instituições democráticas e do Estado de Direito [3].

Para que o Brasil possa ascender à condição de um Estado democrático Digital de Direito, necessário criar e implementar providências relativas à edificação de barreiras eficazes contra a formação de uma unidade (e centralização sem limites e controle) informacional, principalmente no que se refere ao compartilhamento irrestrito de dados pessoais, ao arrepio das exigências do direito fundamental à proteção de dados e da LGPD, assim como em desconsideração às recomendações da ANPD, mais especificamente de seu guia orientativo [4] para o tratamento de dados pessoais pelo poder público. Necessita-se de uma atenção para o emprego de relatórios de impacto de risco, sobretudo de risco algorítmico.

Na condição — aqui advogada — de princípio fundamental estruturante, implicitamente positivado pela CF, a separação/divisão informacional de poderes vincula toda a atuação do Estado brasileiro, devendo ser concretizada pelo legislador, ademais de exigir a motivação das decisões que envolvam todas as formas de tratamento de dados, sobretudo dados pessoais, o que guarda sinergia com o que se extrai das recentes decisões em sede de controle de constitucionalidade exaradas pelo STF.

Tomando como referência o caso do compartilhamento de dados pelo Sistema Brasileiro de Inteligência (Sisbin) com a Agência Brasileira de Inteligência (Abin), o STF, por unanimidade, decidiu [5] que:

1. Os órgãos componentes do Sistema Brasileiro de Inteligência somente podem fornecer dados e conhecimentos específicos à Abin quando comprovado o interesse público da medida, afastada qualquer possibilidade de o fornecimento desses dados atender a interesses pessoais ou privados;

2. Toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário;

3. Mesmo quando presente o interesse público, os dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição não podem ser compartilhados na forma do dispositivo, em razão daquela limitação, decorrente do respeito aos direitos fundamentais;

4. Nas hipóteses cabíveis de fornecimento de informações e dados à Abin, são imprescindíveis procedimento formalmente instaurado e a existência de sistemas eletrônicos de segurança e registro de acesso, inclusive para efeito de responsabilização em caso de eventual omissão, desvio ou abuso [6].

Igualmente digna de nota é a decisão monocrática proferida pelo ministro Gilmar Mendes na ADPF 695 MC/DF, que versa sobre o compartilhamento de dados pessoais pelo Serviço Federal de processamento de Dados (Serpro) com a Agência Brasileira de Inteligência (Abin), com suposto lastro normativo no Decreto nº 10.046, que revogou o Decreto 8.789/19, passando a disciplinar o compartilhamento de dados no âmbito da Administração Pública Federal, ademais de instituir o Cadastro Base do Cidadão (CBC) e criar o Comitê Central de Governança de Dados (CCGD).

Na sua decisão, o ministro afirmou que: *"o regime jurídico de compartilhamento de dados entre órgãos e instituições do Poder Público é matéria de extrema relevância para a proteção constitucional do direito constitucional à privacidade (artigo 5º, caput e incisos X, da Constituição Federal), situando-se como garantia elementar de qualquer sociedade democrática contemporânea"* [7].

Como a coleta e o tratamento de dados pelo Estado é inevitável e mesmo necessária no âmbito do atual cenário de desenvolvimento, indispensável o estabelecimento e afirmação de balizas, éticas, técnicas e jurídicas, pena de configuração do arbítrio. Nesse sentido, vale colacionar o entendimento de Luís Greco:

*"Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao menos em boa parte, como garantia institucional, relativa à própria estrutura da sociedade e do Estado.* ***Nesse nível macro o direito se transforma em uma exigência de separação informacional de poderes****[8]"* (grifos nossos).

A proteção de dados implica, dessa forma, a incorporação definitiva de uma cultura pautada pelos princípios e direitos fundamentais (não só, mas em especial o direito à proteção de dados pessoais, a dignidade da pessoa humana e a autodeterminação informativa) e em sinergia com a LGPD, tarefa que também vincula o Estado brasileiro, que deve estabelecer, mediante a utilização de parâmetros de atuação forjados com base no princípio da separação de poderes, um regime organizacional pautado na divisão por competências, envidando todos os esforços para evitar o compartilhamento abusivo, desproporcional, irrestrito e, portanto, inconstitucional de dados pessoais.

De fato, o direito fundamental à proteção de dados pessoais, assim como se dá com os demais direitos, não se limita à sua dimensão subjetiva na condição de direito de defesa contra intervenções abusivas por parte dos atores estatais, mas exige, para que alcance a necessária efetividade, o acionamento de sua dimensão jurídico-objetiva, que engloba a atuação positiva do Estado também no que diz respeito à garantia da confiabilidade, da integridade e da segurança das infraestruturas técnicas da informação. Isso, por sua vez, resulta em deveres de proteção estatais e em uma correspondente proibição de proteção insuficiente por parte do poder público, em todas as suas formas de manifestação. Nessa senda, importa sublinhar que um dos meios mais eficazes de o Estado concretizar seus deveres de proteção de modo integral é o de garantir o devido processo informacional e a separação informacional de poderes.

A implantação de um Estado democrático Digital de Direito deve ser voltada para o cidadão, mediante a criação e garantia de um ecossistema inovador e suficientemente seguro, transparente e confiável, que minimize os danos e os riscos causados e gerados pelas Tecnologias de Informação e Comunicação e pela Inteligência Artificial (apenas para citar as mais importantes nesse contexto) mediante o recurso às garantias técnicas, éticas e jurídicas orientadas pela proteção e promoção da dignidade da pessoa humana, de sua autodeterminação informacional, da proteção de seus dados pessoais e outros direitos e garantias fundamentais, vedando-se qualquer tipo de prática abusiva, inclusive e principalmente no que diz respeito à segurança cibernética.

O devido processo informacional, contempla, sobretudo os casos envolvendo dados sensíveis, tanto a obrigatoriedade de avaliação preliminar por meio de relatórios de impacto de risco, atendendo aos parâmetros de transparência e de *accountability* durante todo o percurso, quanto o dever de motivação a ser exigido da autoridade competente e responsável pela restrição de direitos fundamentais. No caso do emprego de algoritmos deve-se atentar para a vedação à opacidade e o alcance do direito à explicação, garantindo ainda a auditabilidade, a explicabilidade e a interpretabilidade.

À vista disso, é de se reafirmar que efetividade do princípio (e direito fundamental) do devido processo informacional só será alcançada com o estabelecimento e com a devida concretização da garantia de uma separação informacional de poderes.

Nessa altura, importa relembrar que o STF, como já referido, já se manifestou sobre tais temas em algumas decisões, sobretudo no sentido de uma posição consistente com a ideia da separação informacional de poderes.

A divisão informacional, portanto, configura um limite/fronteira inegociável para o compartilhamento de dados pessoais entre os órgãos da administração pública, atrelando-se à necessidade de compatibilização das finalidades em caso de uso secundário. Daí que a intervenção do Estado não pode comprometer o objetivo e tampouco a finalidade pública que deu ensejo ao processamento, justificando a coleta dos dados pessoais sob pena de desvio de finalidade.

À vista do exposto, resulta mais do que evidente que ainda há muito por fazer para que o devido processo informacional e a separação informacional de poderes tenham a sua dignidade constitucional devidamente afirmada, de modo a, juntamente com outros princípios e direitos fundamentais, servirem de baliza e garante de um Estado Democrático de Direito que mereça ostentar tal título.

Trata-se de tema premente e que carece de maior desenvolvimento legislativo, jurisprudencial e doutrinário, de tal sorte que o que se espera é que com as notas ora lançadas se tenha ao menos logrado contribuir para chamar a atenção para o problema e alguns dos seus respectivos desafios.

[1] CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev*., v. 55, p. 93, 2014. Disponível em: https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4. Acesso em: 4/3/2022.

[2] ROBL FILHO, Ilton Norberto. Alguns apontamentos sobre o constitucionalismo digital. Revista Consultor Jurídico, 22 de janeiro de 2022. Disponível em: https://www.conjur.com.br/2022-jan-22/observatorio-constitucional-alguns-apontamentos-constitucionalismo-digital. Acesso em: 26.02.2022. Sobre o tema, v., ainda, o excelente texto de MENDES, Gilmar Ferreira; OLIVEIRA FERNANDES, Victor. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, Passo Fundo, v. 16, n. 1, p. 1-33, out. 2020. ISSN 2238-0604. Disponível em: https://doi.org/10.18256/2238-0604.2020.v16i1.4103. Acesso em: 28/2/2022.

[3] OCDE. Good practice principles for Data Ethics in the Public Sector, 2020, p. 04. Disponível em: www.ocde.org/digital/digital-goverment/good-practice-principles-for-data-ethics-in-the-public-sector.htm. Acesso em: 26/2/2022.

[4] ANPD. Tratamento de dados pessoais pelo poder público. Guia orientativo. Versão 1.0. janeiro 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 28/2/2022

[5] STF limita fornecimento de dados à Abin. Migalhas, 13 de outubro de 2021. Disponível em: https://www.migalhas.com.br/quentes/353085/stf-limita-fornecimento-de-dados-a-abin. Acesso em: 10/3/2022

[6] Texto extraído do voto da ministra (Disponível em: https://www.internetlab.org.br/wp-content/uploads/2021/10/voto-carmen-lucia-abin-sisbin.pdf. Acesso em: 21/3/2022). Cf., igualmente, a emblemática decisão (Voto conjunto, ADIs 6.389, 6.390, 6.393, 6.388 e 6.387, v. Disponível em: https://www.conjur.com.brhttps://www.conjur.com.br/wp-content/uploads/2023/09/pandemia-reforca-necessidade-protecao-1.pdf. Acesso em: 11/3/2022).

[7] STF, ADPF-MC 695. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15343579920&ext=.pdf. Acesso em: 12/3/2022

[8] Introdução à obra de WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal* : reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Luís Greco (tradução, organização e introdução). Eduardo Viana e Alaor Leite (tradução). São Paulo: Marcial Pons, 2018, p. 45.

**Date Created**
13/05/2022