Schertel e Gasiola: Compartilhamento de dados no setor público

No dia 1º de setembro, o Supremo Tribunal Federal iniciou o julgamento da ADPF 695/DF, proposta pelo PSB, e da ADI 6.649/DF, proposta pela OAB Federal. Ambas as ações questionam o compartilhamento indiscriminado de dados pessoais na Administração Pública Federal, autorizado pelo Decreto 10.046/2019. O julgamento é uma oportunidade de se debaterem os limites constitucionais do fluxo de dados na Administração Pública. As ações ora em pauta permitem a análise de constitucionalidade do decreto à luz da discussão de um caso concreto (trazido pela ADPF), que ilustra de forma impressionante a dimensão do compartilhamento, bem como a falta de transparência e de controle do compartilhamento atual de dados na Administração Pública [1].

O caso diz respeito ao compartilhamento de dados de 76 milhões de brasileiros do Denatran com a Abin, que iria se realizar, com base no Decreto 10.046/2019, após a publicação de extrato de termo de autorização no *Diário Oficial da União*. Na decisão sobre a cautelar, o ministro Gilmar Mendes, relator da ADPF, decidiu que não havia elementos que justificassem a concessão da medida, mas esclareceu que o referido compartilhamento tinha uma grave falha: a impossibilidade de se realizar uma análise de proporcionalidade do referido tratamento, visto que o compartilhamento questionado era despido de medidas de transparência, rastreabilidade ou controle, dado que "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".[2]

Dessa forma, a chave para compreender as fragilidades do Decreto 10.046/2019 reside em analisar os elementos que o tornam incompatível com o regime de proteção de dados estruturado pela Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018) e pela Constituição Federal, que alberga um direito fundamental à proteção de dados (artigo 5, LXXIX), positivado desde a promulgação da Emenda Constitucional 115.

Violação à LGPD

Apesar do âmbito de aplicação da LGPD abranger agentes públicos e privados, o Poder Público está sujeito a um regime jurídico específico de proteção de dados pessoais.[3] Em especial, a estrutura inaugurada pela LGPD de "proibição com reserva" [4] para a legitimidade do tratamento de dadosdeve ser interpretada de acordo com o princípio da legalidade[5] (artigo 37, *caput*, CF), que sujeita as pessoas jurídicas de direito público.

Assim, se os entes públicos estão sujeitos ao princípio da legalidade e o tratamento de dados pessoais é considerado uma interferência no direito fundamental da proteção de dados (artigo 5, LXXIX, CF), este apenas será considerado legítimo se houver uma base legal que o justifique.[6] Isso significa que as hipóteses de tratamento dos artigos 7 e 11 da LGPD precisam ser interpretadas de forma restrita, conforme o princípio da legalidade. Ademais, essa restrição também pode ser extraída das normas específicas para o Poder Público da LGPD, tal qual o artigo 23 e, especificamente para o compartilhamento de dados, nos termos dos artigo 5, XVI e 26, LGPD.

A existência de uma base legal não é a única condição de legitimidade para o compartilhamento de dados pessoais pelo Poder Público. O próprio artigo 26 da LGPD reafirma que o uso compartilhado deve respeitar os princípios de proteção de dados pessoais elencados no artigo 6. Em especial, o compartilhamento deve ser realizado para finalidades específicas[7] (artigo 5, I), de forma transparente (artigo 6, IV) e sendo garantida a responsabilização e prestação de contas pelo agente de tratamento (artigo 6, X).

O Decreto 10.046/2019 estabelece três categorias de compartilhamento — amplo (artigo 11), restrito (artigo 12) e específico (artigo 14) — que são alheias à lógica da proteção de dados pessoais. Isso porque tal norma i) ignora a necessidade de uma base legal para acesso aos dados pessoais pelos órgãos públicos; ii) não estabelece em momento algum a necessidade de especificação das finalidades para as quais os dados serão compartilhados e com quem; iii) não preveem mecanismos de rastreabilidade, tais como convênios ou termos de autorização; e iv) não possibilitam o exercício dos direitos pelos titulares dos dados.

Dessa forma, conclui-se que toda a sistemática de compartilhamento do decreto mostra-se inadequada ao regime jurídico de proteção de dados, seja pela ausência de base legal adequada para a criação do cadastro base e para o seu acesso por outros órgãos interessados, seja pelo fato de ele não estabelecer qualquer instrumento de rastreabilidade e *accountability*, de modo a permitir o controle de sua finalidade e proporcionalidade.

Violação ao direito fundamental à proteção de dados

Com o reconhecimento de um direito fundamental autônomo da proteção de dados pessoais — tanto pela jurisprudência do STF, quanto pela Emenda Constitucional 115 — , cumpre analisar em que medida o Decreto 10.046/2019 está de acordo com a garantia constitucional da proteção de dados.

A existência de um direito fundamental autônomo cujo âmbito de proteção abrange qualquer tratamento de dados pessoais eleva os pressupostos do princípio da legalidade, em especial para o Poder Público. Na medida em que toda operação de tratamento representa uma intromissão no direito fundamental, o Poder Público precisa de uma base legal que justifique. Nesse sentido, o Ministro Gilmar Mendes na ADPF 695 MC/DF entendeu que *"não há uma autorização irrestrita no ordenamento jurídico brasileiro ao livre fluxo e compartilhamento de dados no Poder Público… Desse modo, convênios e acordos de compartilhamento baseados única e exclusivamente nas disposições do Decreto nº 10.046/2019 parecem figurar-se potencialmente lesivo às garantias individuais…".*

Sabe-se que o compartilhamento envolve um risco mais elevado para o direito fundamental à proteção de dados, por diversos motivos. Primeiramente, além de aumentar o número de órgãos ou entes públicos que têm acesso, o compartilhamento de dados em geral está associado a uma mudança de finalidade em relação àquela para a qual os dados foram inicialmente coletados. Essa mudança de finalidade, também identificada muitas vezes com uma mudança de contexto de utilização dos dados, está associada à percepção de danos ao titular, visto que este não tinha expectativa de ter seus dados tratados em contextos diferentes, podendo sofrer consequências negativas a partir de tal mudança.[8]
Ademais, o compartilhamento também pode expor os dados pessoais a riscos de segurança da informação, como vazamentos e acesso não autorizado. Essas características aumentam o risco de uso inadequado e ilegítimo dos dados pessoais e exige maior atenção ao regime jurídico de proteção de dados.

O Tribunal Constitucional Alemão, em uma importante decisão sobre o transmissão de dados entre órgãos públicos, entendeu que a análise de constitucionalidade em casos de compartilhamento funciona como uma porta dupla ("*Doppeltür*").[9] Para que o compartilhamento seja considerado legítimo, deve haver uma base legal que justifique cada uma das operações de tratamento, ou seja, que abra cada uma das portas. Isto é, há que se ter uma base legal para a transmissão de dados e outra base legal para o acesso a eles.

Para além da verificação de uma base legal para cada uma das operações de tratamento, ainda é necessário que essa base legal atenda a determinados critérios, em especial, defina uma finalidade legítima e seja proporcional (de acordo com os testes da adequação, necessidade e proporcionalidade em sentido estrito). Somado a isso, a base legal deve ser clara o suficiente para permitir a análise desses critérios.

O fato de não se conhecerem as finalidades dos compartilhamentos autorizados pelo Decreto 10.046/2019 evidencia a completa impossibilidade de realização da análise da proporcionalidade. Como não se conhecem as finalidades específicas do tratamento —isto é, quando, com quem e para o quê os dados são compartilhados —, não é possível estabelecer se os compartilhamentos realizados são proporcionais, adequados e necessários.[10]

Por fim, a criação do Cadastro Base do Cidadão deveria estar acompanhada de providências procedimentais e organizacionais para diminuir os riscos envolvidos de riscos aos direitos dos titulares. Essas medidas não foram estabelecidas pelo Decreto 10.046/2019 e também não foram executadas de forma adequada pelo Comitê Central de Governança de Dados.

Conclusão
Percebe-se, assim, que para que o compartilhamento de dados na Administração Pública pudesse ocorrer de forma legítima, seria necessário um ato normativo com as salvaguardas previstas na LGPD e que se extraem também do direito fundamental à proteção de dados, o que o Decreto 10.046/2019 nem de longe parece oferecer.

Qualquer sistema que busque viabilizar o fluxo de dados pessoais no âmbito da Administração Pública deve corrigir essas falhas, por meio de medidas básicas que estabeleçam: i) procedimentos de proteção que levem em conta o risco do tratamento de dados pessoais em geral e não apenas de dados sigilosos, especialmente a partir da mudança de finalidade intrínseca a todo compartilhamento; ii) procedimentos especiais que levem em conta o risco do tratamento de dados sensíveis; iii) mecanismos efetivos para o exercício dos direitos do titular, conforme o artigo 18 da LGPD; iv) a edição de ato normativo pelo órgão receptor como requisito para o acesso de dados pessoais, indicando as finalidades para as quais os dados são tratados no âmbito daquele órgão; v) instrumentos de transparência e de *accountability*, que possibilitem o controle do fluxo dos dados pessoais pelo cidadão e pelos órgãos competentes, a exemplo de convênios, atos autorizativos ou outros registros que permitam tal supervisão; vi) a necessidade de realização de relatórios de impacto prévios ao compartilhamento de dados de alto risco; e vii) um sistema de governança mais robusto, para além de um comitê central com composição restrita, conforme previsto no decreto.

Como afirmou Danilo Doneda, na sustentação oral em nome da OAB Federal, *"há diversas formas de sanar as deficiências do decreto, tais como a efetiva verificação de compatibilidade de finalidades nos compartilhamentos, a instituição de medidas de avaliação de risco e 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"*.

O Supremo Tribunal Federal deu um importante passo ao reconhecer um direito fundamental autônomo à proteção de dados no julgamento da ADI nº 6387 em 2020. Com a positivação de tal direito no artigo 5, LXXIX, torna-se basilar concretizar o referido mandamento, impondo limites ao poder informacional da Administração Pública e consolidando uma "separação informacional dos poderes" (*informationelle Gewaltenteilung*), nos termos formulado por Spiros Simitis,[11] Ingo Sarlet e Gabrielle Sarlet concretizam o princípio da separação informacional no direito brasileiro, demonstrando a sua plena aplicabilidade. *"*(…) *o princípio fundamental estruturante, implicitamente positivado pela CF, a separação/divisão informacional de poderes vincula toda a atuação do Estado brasileiro, como norma de eficácia direta e que, dentre outros requisitos, deve ser concretizado pelo legislador e exige a motivação das decisões que envolvam todas as formas de tratamento de dados* (…)"[12]

Se as constituições de forma geral podem ser entendidas como a limitação do poder estatal para a garantia de espaços de liberdade individual e coletiva, o reconhecimento de um direito fundamental à proteção de dados nada mais é do que a limitação do poder informacional, isto é, poder do Estado para coletar, processar e usas informações pessoais dos cidadãos, considerando os riscos de vigilância, discriminação, bem como os danos econômicos dele derivados.

Como afirmou a ministra Rosa Weber na ADI nº 6.387, as normas que estabelecem o tratamento de dados devem *"definir apropriadamente como e para que serão utilizados os dados coletados para, assim, oferecer 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"*.

Nesse sentido, qualquer sistema de compartilhamento de dados no âmbito do Poder Público apenas será legítimo, se contar, em primeiro lugar, com instrumentos de transparência, controle e *accountability* suficientes para evidenciar com quem e para quê os dados são compartilhados; somente então, torna-se possível a realização de um teste de proporcionalidade acerca da finalidade e da necessidade do compartilhamento realizado. É fácil perceber que o Decreto 10.046/2019 está longe de atingir tais requisitos, de onde se extrai a sua inexorável ilegalidade e inconstitucionalidade.

_____

[1] Cf sobre o tema: MENDES, Laura Schertel. Democracia, poder informacional e vigilância, **O Globo** , *Fumus Boni Iuris*.

[2] Decisão, Medida Cautela na ADPF 695/DF, fl. 41.

[3] Cf. Gasiola, Gustavo Gil; Machado, Diego; Mendes, Laura Schertel. A Administração Pública entre a transparência e a proteção de dados. Revista de Direito do Consumidor, vol. 135, 2021, p. 5.

[4] De acordo com essa estrutura normativa, denominada na doutrina alemão de "*Verbot mit Erlaubnisvorbehalt*", o tratamento de dados apenas seria permitido com uma base legal ou através da legitimação pelo próprio titular. Cf. BUCHNER, Benedikt. Grundsätze des Datenschutzrechts. In: TINNEFELD, Marie-Theres; BUCHNER, Benedikt; PETRI, Thomas; HOF, Hans-Joachim. Einführung in das Datenschutzrecht, 8ª ed. Berlin: De Gruyter, 2018, p. 234.

[5] Nesse sentido, cf. REIMER, Phillip. Verwaltungsdatenschutzrecht. Baden-Baden: Nomos, 2019, p. 76-77; e GRIMM, Dieter. Der Datenschutz vor einer Neuorientierung. JZ, n. 12 ano 68, 2013, p. 587.

[6] Em sentido semelhante, cf. WIMMER, Miriam. O regime jurídico do tratamento de dados pessoais pelo Poder Público. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JR., Otavio Luiz (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021, p. 291.

[7]

Elencando a finalidade específica como uma das condições do uso compartilhado de dados de acordo com o Art. 26, cf. TASSO, Fernando Antonio. Compartilhamento de dados entre o setor público e privado – possibilidades e limites. Revista do Advogado, n. 114, 2019, p. 112.

[8] Cf. NISSENBAUM, Helen. Privacy in context. Stanford: Stanford University Press, 2010, p. 216.

[9] Cf. BVerfGE 130, 151; BVerfGE 155, 119. No caso, o Tribunal Constitucional Alemão entendeu como inconstitucional o dispositivo da lei alemã de telecomunicações (Telekommunikationsgesetz) que previa o compartilhamento de dados das empresas de telecomunicação com os órgãos de segurança. Isso, porque o legislador teria criado uma base legal suficiente apenas para justificar o envio dos dados, mas não o recebimento deles pelos órgãos de segurança.

[10] STF, ADI n. 6387, 6388, 6389, 6393, 6390/ DF, Rel. Min. Rosa Weber, Caso IBGE.

[11] SIMITIS, Spiros. Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung. NJW 1984, p. 394-405.

[12] SARLET, Ingo; SARLET, Gabrielle. Separação informacional de poderes no Direito Constitucional brasileiro / Ingo Wolfgang Sarlet, Gabrielle Bezerra Sales Sarlet. – São Paulo: Associação Data Privacy Brasil, 2022

Meta Fields