

STF e o compartilhamento de dados no âmbito do poder público

Para entender a questão do compartilhamento de dados no âmbito do poder público brasileiro, cumpre iniciar recordando o novo sistema de publicidade, de transparência, de eficiência e, sobretudo, de responsabilização erigido a partir da Constituição Federal de 1988 (doravante CF/88). De forma mais explícita, em razão da posição central da pessoa humana e de sua proteção integral, vários dispositivos foram erigidos na consagração de balizas e fronteiras de atuação do Estado federal, indo além dos



Ingo Sarlet
advogado e professor

Dentre eles, v.g., o artigo 37, que contempla os principais princípios da

administração pública brasileira, formatou um Estado vocacionado a servir o cidadão, inclusive e cada vez mais no que diz respeito à transformação digital e seus desafios. Nesse contexto, destaca-se o fato de o Estado, para uma adequada e eficaz criação e execução das políticas públicas, necessitar de acesso a um número crescente e diversificado de dados.

Dada a sua relevância não apenas para a compreensão do conteúdo e do alcance do direito fundamental à proteção de dados na CF, mas também para efeitos de seu diálogo com a legislação, jurisprudência e mesmo doutrina sobre o tema, importa sublinhar que diversos diplomas legais em vigor já dispõe sobre aspectos relevantes da proteção de dados, destacando-se aqui o Código de defesa do consumidor (Lei 8.078/1990), a Lei de Acesso à Informação (Lei 12.527/2011), o assim chamado Marco Civil da Internet (Lei 12.965/2014) e o respectivo Decreto que o regulamentou (Decreto 8.771/2016), mas, especialmente a LGPD (Lei 13.709/2018).

Por se tratar de normativa recentemente submetida ao crivo do STF, no âmbito das ações de controle concentrado referidas no título da presente coluna (ADI 6.649 e ADPF 659, da relatoria do ministro Gilmar Mendes, julgadas recentemente, em 15/9/2022) merece destaque particular o Decreto 10.046/2019. Antes contudo, de comentar o citado julgamento, há que situar a sua questão de fundo, no contexto mais amplo do sistema protetivo de dados pessoais no Brasil, ainda na sua fase inicial de desenvolvimento.

Nessa perspectiva, é mais do que consolidado, tanto na esfera do discurso acadêmico, quando ao nível legislativo e jurisprudencial, em especial mirando a trajetória mais antiga e tradicional do ambiente europeu, mas também já em boa parte recepcionada no Brasil, particularmente desde a entrada em vigor da LGPD e do reconhecimento pelo STF e posterior inclusão no texto da CF/88 de um direito fundamental à proteção de dados pessoais, que a coleta, tratamento, mas em especial o uso e compartilhamento de tais dados não pode ser abusivo, devendo obediência a uma série de parâmetros estabelecidos pela ordem jurídico-constitucional. Isso se revela ainda mais evidente quando se trata de dados em poder dos órgãos estatais, num ambiente de hiper vigilância.

Nessa medida, o foco está na concretização do marco normativo constitucional, inclusive no que diz respeito às limitações estruturais e substantivas ao Estado brasileiro [\[1\]](#), de modo a guardar consistência não apenas (embora primacialmente) com a dignidade da pessoa humana e os direitos e garantias fundamentais, mas igualmente com as exigências do Estado Democrático de Direito (artigo 1º, CF), da separação de poderes e sua respectiva divisão funcional (artigo 2º, CF), os objetivos fundamentais do Estado brasileiro (artigo 3º, CF), dos princípios que regem as relações internacionais (artigo 4º) e do Estado federal, de modo a atuar como garante do sigilo, da confiança e da transparência, que são de capital importância para um devido processo informacional [\[2\]](#).

É também nesse contexto que assume relevância o reconhecimento de um princípio fundamental estruturante e implicitamente positivado pela CF, o assim chamado princípio (e correspondente dever) da separação/divisão informacional de poderes, que vincula toda atuação estatal, 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, sobretudo dados pessoais, para a configuração efetiva de uma proteção multinível [\[3\]](#) da pessoa humana na sociedade informacional, o que, ademais disso, guarda sinergia com o que se extrai das recentes decisões em sede de controle de constitucionalidade exaradas pelo STF [\[4\]](#).

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: os órgãos componentes do Sisbin 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; Toda e qualquer decisão de fornecimento desses dados deverá ser devida e formalmente motivada para eventual controle de legalidade pelo Poder Judiciário; 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; 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 [\[6\]](#).

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). Naquela 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"* [\[7\]](#).

Recentemente, em sede de decisão definitiva, o ministro Gilmar Mendes, relator dos feitos, julgou parcialmente procedentes a ADI 6.649 e a ADPF 695 para conferir interpretação conforme à normas veiculadas pelo Decreto 10.046/2019, no que foi acompanhado pela maioria dos ministros que participaram do julgamento.

Segundo se extrai do voto do ministro Gilmar Mendes, o compartilhamento de dados passa a ter cada vez uma posição central na atuação do Estado, sobretudo no que se refere às políticas públicas, de tal sorte que pressupõe a conformidade com a LGPD, notadamente do ponto de vista da indicação de propósitos legítimos, específicos, e explícitos para todas as etapas do tratamento. Assim, as finalidades primárias e secundárias, caso necessário, devem ser devidamente compatibilizadas, vez que o compartilhamento, em si, deve ser restrito ao mínimo e balizados pelo cumprimento dos requisitos, das garantias e dos procedimentos legais.

Extraí-se ainda do voto proferido, que o compartilhamento dos dados pessoais entre os órgãos públicos exige o enquadramento no que dispõe o artigo 23, I, da LGPD, notadamente quanto à publicidade das hipóteses nas quais cada entidade governamental compartilha ou tem acesso aos dados. Em suma, o entendimento do ministro Relator foi de que o acesso de órgãos e de entidades governamentais ao Cadastro Base do Cidadão fica condicionado ao que outrora foi referido.

Outro ponto relevante diz com as competências do Comitê Central de Governança de Dados, na medida em que, segundo o relator, deveriam ser restringidas às que foram expressas no artigo 21, incisos VI, VII e VIII do Decreto 10.046/2019, desde que se atue no estabelecimento e na prevenção de mecanismos rigorosos no controle de acesso ao Cadastro Base do Cidadão, ou seja, dito de outro modo, que os órgãos e entidades públicas têm o dever de demonstrar a real necessidade de acesso e de compartilhamento dos dados. Para tanto — ainda de acordo com o que se extrai do voto —, a referida permissão somente deverá ser concedida para que sejam alcançados propósitos legítimos, específicos e explícitos, sendo limitada às informações que sejam indispensáveis ao atendimento do interesse público, nos termos do artigo 7, III, bem como do artigo 23, caput, I da Lei 13.709/2018.

Além disso, para fins de compartilhamento de dados, foi estabelecida a obrigação de formulação de uma justificativa prévia e minudente, baseada no emprego da proporcionalidade, da razoabilidade e da principiologia da LGPD, tanto para a necessidade de inclusão de novos dados pessoais na base integradora, quanto no que toca à escolha das bases temáticas do Cadastro Base do Cidadão [\[8\]](#).

O ministro relator orienta, outrossim, a adoção de medidas de segurança, designadamente, de um sistema eletrônico de registro de acesso para efeitos de responsabilização em casos abusivos. Agrega, ainda, que o compartilhamento nas atividades de inteligência deve seguir os critérios estabelecidos em legislação própria, bem como parametrizados pela decisão do STF no já analisado caso envolvendo a Abin. Importa destacar, na mesma toada, a reponsabilidade civil do Estado pelos danos causados aos particulares em consonância com a dicção do artigo 42 e seguintes da LGPD, inclusive com o direito de regresso contra os servidores e agentes públicos responsáveis pelo ato ilícito, em caso de culpa ou de dolo.

Importante reafirmar, ainda sobre a decisão ora comentada, que de acordo com o julgado, a transgressão dolosa ao dever de publicidade estabelecido no artigo 23, I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por ato de improbidade administrativa.

Ne mesma esteira é de se sublinhar que o STF, com efeitos *pro futuro*, declarou a inconstitucionalidade do artigo 22 do Decreto 10.046/19, preservando, no entanto, a atual estrutura do Comitê Central de Governança de Dados pelo prazo de sessenta dias a contar da data da publicação da ata de julgamento. Agrega-se aqui que tal prazo deveria ser adequado de modo a permitir que o chefe do Executivo atue no sentido de atribuir ao órgão a independência, a autonomia e a pluralidade necessária, bases inarredáveis para a sua legitimidade constitucional e operação conforme ao Estado Democrático de Direito.

Nessa altura, não custa lembrar que, a Organização para Cooperação e Desenvolvimento Econômico (OCDE), reafirmou, a despeito da posição brasileira no ranking dos países com alto grau de digitalização, a urgência quanto a uma ampla modificação na atuação do Estado brasileiro no concernente à superação da desigualdade, da diminuição dos custos e na ampliação da rede de fornecimento de serviços essenciais, garantindo e expandindo o acesso à internet [\[9\]](#), bem como do fortalecimento de parcerias entre as empresas e o governo, da educação para a cidadania digital, ademais da necessidade de se garantir a independência da ANPD e fortalecer o papel do Conselho Nacional de Proteção de Dados e da Privacidade, assim como apostar na implementação de políticas públicas pautadas na transparência e na confiança.



Além disso foi recomendada a adoção de outras medidas, tais como: a criação de uma ampla comunidade de líderes digitais nos setores público e privado, acadêmico e sociedade civil para implementar a Estratégia Nacional de Segurança Cibernética; O desenvolvimento de ferramentas para avaliar a implementação da estratégia, avaliar o progresso e revisar os objetivos adequadamente; O aumento do orçamento para a implementação da Estratégia Nacional de Segurança Cibernética, definindo marcos claros e mensuráveis; A promoção de uma abordagem descentralizada quanto à governança da segurança digital, com ministérios e órgãos liderando suas áreas de competência e o GSI/PR como coordenador, aprimorando os conhecimentos sobre segurança digital no governo; A implementação de campanhas de conscientização entre empresas, indivíduos e dentro do governo; O fortalecimento dos programas de treinamento e educação em segurança digital em todos os níveis, a criação de um registro nacional de instrutores em segurança digital e o encorajamento dos estudantes para que sigam carreiras na área da segurança digital; O incremento substancial do diálogo multilateral sobre segurança digital, com base no modelo brasileiro de governança da Internet (CGI) [10].

À vista de todo o exposto, é possível, à guisa de conclusão, afirmar que, a despeito de significativa evolução no campo da proteção de dados, em especial no que diz respeito ao estabelecimento, com destaque aqui para o STF, de critérios a balizarem o compartilhamento de dados a possibilidade de seu controle, inclusive no plano jurisdicional, dando assim os primeiros passos rumo ao estabelecimento de um sistema de separação informacional de poderes e de um devido processo informacional, muito ainda há o que fazer, sendo imensos, complexos e diferenciados os problemas e desafios a enfrentar e equacionar.

Tendo em conta a recente evolução na jurisprudência do STF, bem como, entre outros, do trabalho competente já levado a efeito — em que pese seu curto tempo de existência e ainda grandes limitações em termos de recursos financeiros e humanos — pela ANPD, há fundadas razões para sermos otimistas. A esperança, é claro, que tais expectativas venham gradualmente a se concretizar em ritmo cada vez maior.

[1] LOUREIRO, Bernardo Pacheco. *Publicadores de dados: da gestão estratégica à abertura*. São Paulo: Open Knowledge Brasil, 2021.

[2] DI FABIO, Udo. *Grundrechtsgeltung in digitalen Systemen: Selbstbestimmung und Wettbewerb im Netz*. München: C.H. Beck, 2016, p. 44-45; V. ainda BIONI, Bruno; MARTINS, Pedro. Devido processo informacional: um salto teórico-dogmático necessário?, Manuscrito. Disponível em: <https://brunobioni.com.br/wp-content/uploads/2020/08/Ensaio-Devido-Processo-Informacional1.pdf>. Acesso em: 2/9/2022

[3] TRIBUNAL decide que Sistema de Indicação de Risco viola direitos humanos. InternetLab, 2020. Disponível em: <https://internetlab.org.br/pt/itens-semanario/holanda-tribunal-decide-que-sistema-de-indicacao-de-risco-viola-direitos-humanos/>. Acesso em: 11 mar. 2022. 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.

[4] Cf. Voto Ministra Cármen Lúcia acerca do compartilhamento de dados e de informações pela Abin (Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2021/10/voto-carmen-lucia-abin-sisbin.pdf>. Acesso em: 21 mar. 2022). No voto, a ministra afirmou: "A Constituição da República repudia poder sem controle, exige a motivação dos atos administrativos e que todos eles se guiem pelos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. As atividades de inteligência, ainda que acobertadas pelo sigilo, se submetem ao escrutínio externo dos demais Poderes (Legislativo e Judiciário), devendo ser afastada qualquer interpretação que dê margem a arbitrariedades".

[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 mar. 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 mar. 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.pdf>. Acesso em: 11 mar. 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] STF, ADI 6.649/DF e ADPF 695. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6079238>. Acesso em: 9/10/2022

[9] A pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros — TIC domicílios 2020 —, publicada em 25/11/2021, pelo Comitê Gestor da Internet no Brasil mostra que há muito ser feito em termos de infraestrutura e acesso às Tecnologias de Informação e Comunicação (TICs), especialmente quanto ao acesso (quase 1/5 dos domicílios brasileiros não têm acesso à internet) e quanto à inclusão e habilidades digitais, já que o telefone celular é o principal dispositivo de acesso à rede para 99% da população usuária, parcela da qual mais da metade manuseia-o exclusivamente para acessar à internet (esse uso exclusivo chega a três quartos no Nordeste), tudo isso levando em consideração também o custo e as desigualdades de educação, raça/cor, gênero e renda.

[10] OECD. A Caminho da Era Digital no Brasil, OECD Publishing, 2020. Disponível em: <https://doi.org/10.1787/45a84b29-pt>. Acesso em: 2. out. 2022.

Meta Fields