

ADI 7.896: proteção de dados pessoais, soberania digital e papel do Estado

17/05/2026

Em 22 de fevereiro de 2026, o ministro Flávio Dino, do STF (Supremo Tribunal Federal), determinou a suspensão do processo de desestatização da Celepar (Companhia de Tecnologia da Informação e Comunicação do Paraná), no âmbito da Ação Direta de Inconstitucionalidade 7.896 [1]. O pleito é extremamente complexo e tensiona tanto a [Lei Geral de Proteção e Dados Pessoais \(LGPD\)](#) quanto o próprio Direito Administrativo. Dessa forma, sem a pretensão de esgotar todas as camadas do caso, propõe-se considerações a partir de dois eixos: (i) a **proteção de dados pessoais**; e (ii) a **soberania digital e o papel do Estado na sociedade digitalizada**.

Sobre o tópico de **proteção de dados pessoais**, o caso gravita em torno do artigo 4º, inciso III, da [LGPD](#), em conjunto com o §2º e §4º do mesmo artigo. A partir da leitura dos dispositivos elencados, nota-se que a [LGPD](#) autorizou o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais por parte de pessoas jurídicas de direito privado, contanto que haja tutela de pessoa jurídica de direito público e que não haja a transferência da totalidade dos dados pessoais que compõem o banco, observando-se, ainda, legislação específica, os princípios gerais de proteção e os direitos do titular previstos na LGPD. Essa é uma análise de legalidade, ontológica.

O ministro Flávio Dino, a partir de uma leitura da proteção de dados pessoais como direito fundamental, incluído pela Emenda Constitucional nº 115/2022, demonstrou preocupação com a “(...) ausência de balizas normativas claras sobre o controle e o tratamento dos dados pessoais sensíveis, bem como daqueles inseridos na ressalva do inciso III do art. 4º, da LGPD” [2], razão pela qual determinou a suspensão do processo de desestatização da Celepar, de forma que o Estado do Paraná mantenha controle sobre as “(...) bases de dados pessoais sensíveis e classificados no rol do art. 4º, III, da LGPD, vedada a sua transferência integral a entes de natureza privada, exceto na hipótese em que o capital seja integralmente constituído pelo Estado;” [3], bem como elabore Relatório de Impacto de Proteção de Dados Pessoais, entre outras medidas.

Em primeiro lugar, há de se ter em vista que tal decisão, monocrática, ocorreu em sede de cognição sumária, com base na livre convicção do ministro de que as informações eram



insuficientes para uma tomada de decisão segura sobre um direito fundamental. Feita a ressalva, é importante acompanhar os desdobramentos da ação para se verificar qual o entendimento da Corte Constitucional sobre uma nova hipótese de tratamento exclusivo nos termos do artigo 4, § 4º, isto é, se tal vedação alcança não só as finalidades de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, mas também dados pessoais sensíveis, que possuem grande potencial de discriminação e lesão aos titulares [4]. Se a decisão do STF seguir essa linha, haverá prestígio ao direito fundamental à proteção de dados pessoais, com maior rigor para o tratamento de dados pessoais sensíveis, mas poderá impactar o processo de adaptação dos entes federativos com base no parâmetro legal até então posto.

Relatório de riscos

O segundo ponto relaciona-se com a necessidade de realização de Relatório de Impacto à Proteção de Dados Pessoais, instrumento previsto em lei para descrever os “(...) os tratamentos de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” [5], cuja regulamentação está prevista na Agenda Regulatória da Agência Nacional de Proteção de Dados Pessoais (ANPD) para o biênio 2025-2026 [6]. Tal instrumento é salutar para que o STF tenha subsídios para analisar, com o apoio técnico da ANPD, que figura como *amicus curiae*, exatamente o que será realizado com os dados pessoais nesse processo de desestatização, bem como os riscos envolvidos.

Contudo, a discussão precisa avançar para além do arcabouço regulatório existente para um debate sobre a **soberania digital** e qual o **papel do Estado na sociedade digitalizada**, em que os dados pessoais figuram no centro do que se denominou como Quarta Revolução Industrial [7], em um processo de constante dataficação da sociedade, isto é, o funcionamento da sociedade com base nos dados, com impacto no comportamento das pessoas, em como o mercado opera e nas funções do governo [8].

É nesse âmbito de novas formas de comunicação e digitalização que surgiram modelos de negócios centrados no tratamento de dados pessoais, a exemplo das grandes plataformas digitais[9], cenário em que as “Empresas tecnológicas possuem maior acesso aos dados dos cidadãos que Governos” [10], enquanto os titulares permanecem desavisados de como os seus dados são tratados. Controlar dados, infraestruturas e conhecimentos relacionados à inteligência artificial, por exemplo, são preocupações relacionadas com o “[...] cenário da geopolítica e da economia atual” [11].

Mesmo considerando o marco legal e regulatório em construção no país, como o [Marco Civil da Internet](#), a própria LGPD, o [Estatuto Digital da Criança e do Adolescente](#), discussões de regulação sobre inteligência artificial ([Projeto de Lei nº 2.338, de 2023](#)), bem como políticas governamentais como a Estratégia Nacional de Governo Digital ([Lei nº 14.129, de 2021](#)) e o Plano Nova Indústria Nacional, a doutrina aponta cenário preocupante em termos de soberania e controle de dados pessoais. Órgãos e entidades do Estado brasileiro, em diversos poderes e instâncias federativas, adotam soluções tecnológicas de empresas estrangeiras que implicam em transmissão de dados pessoais e estratégicos, armazenados em diversos lugares do mundo

[12]. Embora tais contratações possam ser, em um primeiro momento, economicamente mais vantajosas, não podemos cair na armadilha do ‘eficientismo’ e esquecer de outros valores constitucionalmente previstos [13].

Tal preocupação se agrava face a existência de legislação estadunidense, *The Clarifyng Lawful Overseas Use of Data (Cloud) Act*, que autoriza autoridades a acessar dados pessoais tratados por empresas estadunidenses, mesmo que tais dados estejam fora do território dos Estados Unidos. Tudo isso em um cenário de aplicação de sanções a autoridades brasileiras e ingerência externa nos assuntos nacionais, particularmente relacionados às iniciativas de regulação de grandes plataformas.

É nesse contexto que se insere o tema da soberania digital, conceito relacionado com a autonomia de uma nação ou região sobre decisões relacionadas ao ambiente digital, infraestruturas digitais e desenvolvimento tecnológico, com preocupações contemporâneas crescentes sobre segurança nacional e jurisdição, autonomia econômica e desenvolvimento e proteção de direitos, notadamente àqueles relacionados à proteção de dados pessoais [14].

Diante de nós surge uma escolha: (1) permanecer na condição de consumidores de tecnologias alimentadas com nossos próprios dados, perpetuando uma lógica de desigual divisão internacional de trabalho [15], com o comprometimento da soberania digital, ou (2) repensar a presença digital do Estado, reestruturar o marco regulatório, desenvolver infraestrutura digital e adotar a postura de dados pessoais como um ativo estratégico para se assegurar o desenvolvimento do mercado interno e a consolidação de direitos humanos [16].

Daí a importância das obras de Mariana Mazzucato [17], que nos revelam que a retirada do Estado de setores estratégicos ocasiona a diminuição de sua capacidade de inovar, acumular aprendizado, implementar políticas públicas e resolver problemas complexos, como aqueles relacionados à área tecnológica. Urge reformular o papel do Estado para além de um “(...) *agente passivo de regulação de mercado, mas como um agente ativo e orientado para uma missão, capaz de moldar e cocriar valor público diante de desafios sociais complexos*” [18]. É necessário rememorar a função do Estado como catalisador de transformações [19], para induzir a transformação digital e aprimorar a infraestrutura pública nacional, a partir, por exemplo, de uma revisão da governança das empresas estatais para um planejamento orientado por missões [20].

Convém aproveitar o momento em que a proteção de dados pessoais se encontra no centro do debate jurídico e institucional para avançar nas discussões sobre a soberania digital do país, de forma pragmática, para além da soberania utilizada como argumento ou discurso [21]. Se esse é o caminho que o país escolher, será necessário reestruturar nosso marco regulatório e repensar o papel do Estado na atual sociedade, para que possa promover o desenvolvimento e assegurar direitos fundamentais, como um país soberano.

[1] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 7.896/PR**. Relator: Min. Flávio Dino. Decisão de 22 fev. 2026. Brasília, DF: Supremo Tribunal Federal, 2026. Disponível [aqui](#). Leia a íntegra da decisão [aqui](#).



[2] *Ibid*, p. 21-22.

[3] *Ibid.*, p. 22.

[4] VENTURINI, Otávio; OLIVEIRA, Gustavo Justino de; GLASSMAN, Guillermo. Vazamento de dados sensíveis de HIV/AIDS e a responsabilização do Estado. **CartaCapital**, 02 out. 2025. Disponível [aqui](#).

[5] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**: Seção 1, Brasília, DF, 15 ago. 2018, art. 5, inc. XVII.

[6] BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 31, de 22 de dezembro de 2025. Altera a Agenda Regulatória para o biênio 2025-2026. **Diário Oficial da União**: Seção 1, Brasília, DF, p. 858, 24 dez. 2025.

[7] SCHWAB, Klaus. **The Fourth Industrial Revolution**. Nova York: Portfolio Penguin, 2017.

[8] TAVARES, André Ramos. **A nova Matrix: Direito (re)programando na sociedade plataformizada**. São Paulo: Etheria, 2024. No mesmo sentido: CUKIER, Kenneth; MAYER-SCHÖENBERGER, Viktor. *The Rise of Big Data: How It's Changing the Way We Think About the World*. **Foreign Affairs**, v. 92, n. 3, p. 28-40, May/June 2013. Disponível [aqui](#).

[9] *Ibid*.

[10] Tradução livre. WORLD ECONOMIC FORUM. **The Global Risks Report 2025**. Genebra: World Economic Forum, jan. 2025, p. 38. Disponível [aqui](#).

[11] SILVEIRA, Sérgio Amadeu da. Prefácio. In: LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos (orgs.). **Economia política de dados e soberania digital: conceitos, desafios e experiências no mundo**. Avaré: Editora Contracorrente, 2025. p. 9 - 14, p. 10.

[12] MATOS, M. G. P.; LEMOS, C; ARROIO, Ana. Panorama e perspectivas do Brasil e a Economia de Dados. In: LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos (orgs.). **Economia política de dados e soberania digital: conceitos, desafios e experiências no mundo**. Avaré: Editora Contracorrente, 2025. p. 439-480. No mesmo sentido: ARROIO, Ana. A economia política de dados na perspectiva dos (B)RICS. In: LASTRES, Helena Maria Martins; CASSIOLATO, José Eduardo; DANTAS, Marcos (orgs.). **Economia política de dados e soberania digital: conceitos, desafios e experiências no mundo**. Avaré: Editora Contracorrente, 2025. p. 235-272. GROHMANN, Rafael; COSTA BARBOSA, Alexandre. Sovereignty-as-a-service: how big tech companies co-opt and redefine digital sovereignty. **Media, Culture & Society**, London, v. 47, n. 3, p. 1-18, 2025.

[13] OLIVEIRA, Gustavo Justino de; ZACCARIOTTO, Caio Augusto Santos. O efficientismo administrativo e seu remédio. **Consultor Jurídico**, 12 out. 2025. Disponível [aqui](#). No mesmo sentido: MAZZUCATO, Mariana. *Efficiency at what and for whom? How DOGE represents the latest chapter in the fifty year project to dismantle the state*. **Mission Economics**, 1 ago. 2025. Disponível [aqui](#).

- [14] POHLE, J.; THIEL, T. Digital sovereignty. **Internet Policy Review**, 9(4). 2020. Disponível [aqui](#).
- [15] BELLI, L.; JIANG, M. Conclusion: digital sovereignty in the BRICS: structuring selfdetermination, cybersecurity, and control. In: JIANG, M.; BELLI, L. (Ed.). **Digital sovereignty in the BRICS countries: how the global South and emerging power alliances are reshaping digital governance**. Cambridge: Cambridge University Press, 2025. p. 214-238. No mesmo sentido: SILVEIRA, Sérgio Amadeu da, *Op cit.*.
- [16] TAVARES, André Ramos, *op. cit.*.
- [17] MAZZUCATO, Mariana; KATTEL, Rainer. Market-Shaping States: A new theory of public sector capacities and capabilities. UCL Institute for Innovation and Public Purpose, **Working Paper Series** (IPP WP 2026-03). Disponível [aqui](#). Acesso em: 28 fev. 2026. No mesmo sentido: Mazzucato, *op. cit.*. MAZZUCATO, Mariana (ed.). **State Transformation in Brazil: Designing mission-oriented public procurement, state-owned enterprises and digital public infrastructure to advance sustainable and inclusive growth**. UCL Institute for Innovation. Londres: UCL Institute for Innovation and Public Purpose, Policy Report 2024. Disponível [aqui](#).
- [18] Tradução livre. *Ibid.*, p. 18.
- [19] GOMIDE, Alexandre; LOTTA, Gabriela. Building Resilience, Agility, and Trust: The Neo-Weberian State as a Referential Model for Brazilian Public Administration. **Journal of Policy Studies**, v. 39, n. 3, p. 45-55, Sep. 2024. DOI: 10.52372/jps39304. Acesso em: 15 nov. 2025.
- [20] MAZZUCATO, Mariana (ed.), *op cit.*.
- [21] GROHMANN, Rafael; COSTA BARBOSA, Alexandre. Sovereignty-as-a-service: how big tech companies co-opt and redefine digital sovereignty. **Media, Culture & Society**, London, v. 47, n. 3, p. 1-18, 2025. No mesmo sentido: SANTANIELLO, Mauro. Attributes of digital sovereignty: a conceptual framework. **Internet Policy Review**, Berlin, v. 13, n. 1, p. 1-21, 2024.

Fonte: <https://conjur.jumps.com.br/2026-mai-17/adi-7-896-protecao-de-dados-pessoais-soberania-digital-e-papel-do-estado/>